CYSMICS Picks Workshop

8:30 - 9:00 AM	Registration and Networking
9:00 - 9:15 AM	Directors Welcome
9:15 - 9:40 AM	**Fabian Boemer** and **Ro Cammarota**, Intel AI Research *Trends in AI with Privacy and Security*
9:40 - 10:05 AM	**Ahmad-Reza Sadeghi**, TU Darmstadt *CYSEC in CYSMICS*
10:05 - 10:30 AM	**Azalia Mirhoseini**, Google Brain *Machine Learning for Systems*
10:30 - 10:45 AM	Break
10:45 - 11:10 AM	**Farinaz Koushanfar**, UC San Diego *MICS in CYSMICS*
11:10 - 11:35 AM	**Luca Davi**, Un of Duisburg-Essen *Protecting Existing Smart Contracts Against Attacks*
11:35 AM - 12:00 PM	**Kamalika Chaudhuri**, UC San Diego *Challenges in Privacy-preserving Data Analysis*
12:00 - 12:35 PM	Lunch and Networking
12:35 - 1:00 PM	**Srdjan Capkun**, ETH Zurich Foundation *Secure Execution and It's Applications*
1:00 - 1:25 PM	**Hadi Esmaeilzadeh**, UC San Diego *Accelerating Intelligence: An Edge to Cloud Continuum*
1:25 - 1:50 PM	**Gene Tsudik**, UC Irvine *IoT Security*
1:50 - 2:15 PM	Panel: Top Picks in Real World AI Security and Privacy Moderator: **Ahmad-Reza Sadegh** (TU Darmstadt) Panelists: **Srdjan Capkun** (ETHZ), **Tara Javidi** (UC San Diego), **Casimir Wierzynski** (Intel AI Research), **Azalia Mirhosein**i (Google Brain)
2:15 - 3:00 PM	Open Discussions and Networking