Contribution ID: **6** Type: **Talks**

Ten simple rules for evaluating the security of research software

Software security is a familiar concept to anyone using digital devices, often highlighted by frequent and annoying prompts for urgent software updates. When it comes to research software, security takes greater significance: researchers are often working on confidential projects and handling sensitive research data such as personal data. When it comes to security, researchers, who often depend on externally developed tools, are faced with a dilemma: turn to their local overworked IT-security teams to thoroughly assess the security of their code and pipelines or hope that the software libraries and tools they are using are not exposing their confidential projects to the public internet, or undermining the integrity of their files and computer systems. In this talk, we propose a set of rules that researchers can use to self assess the security of the research software they use. After outlining a framework for identifying the potential level of risks, we showcase examples and solutions when it is mandatory to make sure that there are no data leaks, no unwanted access by others, no data corruption. We hope that our proposed checklist will grow and adapt, becoming a living document that provides ongoing value to the research software community.

Primary author: GLEREAN, Enrico

Co-authors: BAST, Radovan; DARST, Richard (Aalto University)

Presenters: GLEREAN, Enrico; BAST, Radovan; DARST, Richard (Aalto University)

Track Classification: Track 1