Contribution ID: **54** Type: **Presentations**

Challenges for Data Loss Prevention at Research Infrastructures

Thursday, 30 November 2017 16:45 (15 minutes)

Data Loss Prevention (DLP) is a classic but, currently, often overlooked security domain. DLP aims to identify and restrict access to non-public information, such as Personally Identifiable Information (PII) or confidential information. DLP covers data in rest, data in transit and data in use and also requires procedures and tools to monitor how DLP is implemented.

Researchers, research institutions, and research infrastructures handle a rapidly increasing amount of PII and confidential information, due to digitalization. Compared with IT services where the format of data and data transfer is strictly defined, e.g. the financial sector, DLP at Research infrastructures is a formidable challenge due the formidable spectrum of formats and platforms for the data. The complexity of research related DLP is increased by the autonomous and dynamic nature of research, the sometimes unclear responsibilities on accountability for DLP, and last but not least, the growing amount of PII in research environments that have originally been designed for handling public scientific data.

Many commercial tools available for DLP are not always feasible for research infrastructures for the reasons mentioned above. In addition, pricing can make the current commercial DLP applications out of reach for the research community. Instead, jointly developed open source based software and common services to ensure DLP, could provide a feasible roadmap for research.

Additional pressure on implementing satisfactory management and technical controls for DLP comes from the General Data Protection Regulation (GDPR) with urges for compliancy with requirements for user consent, right to erasure, security of processing of PII, and privacy by design. As joint projects with private industry is on the increase, pressure to implement DLP for information protected by non-disclosure agreements is also increasing.

In our presentation, we aim to pinpoint the current state of DLP at Research Infrastructures, to identify the most urgent challenges, and suggest a sustainable roadmap on how the research infrastructures can jointly implement measures for adequate DLP. We will discuss available operational solutions to implement and monitor DLP. We will also highlight the community driven policy frameworks developed through WISE (Wise Information Security for collaborating E-infrastructures) that guide infrastructures to developing suitable environments to address DLP.

Topic Area

Security, trust and identity

Type of abstract

Presentation (15 minutes)

Primary author: KAILA, Urpo (CSC)

Co-authors: SHORT, Hannah (CERN); Ms HARRIS, Nicole (GÉANT)

Presenter: KAILA, Urpo (CSC)

Session Classification: Security, trust and identity management