Contribution ID: **109** Type: **Oral**

The future of academic computing security

Thursday 13 October 2016 12:15 (15 minutes)

This presentation offers an overview of the current security landscape - the threats, tools, techniques and procedures followed by attackers. These attackers range from cybercriminals aiming to make a profit, to nation-states searching for valuable information. Threat vectors have evolved in recent years; focus has shifted significantly, from targeting computer services directly, to aiming for the people managing the computational, financial and strategical resources instead. The academic community is at a crucial time and must proactively manage the resulting risks. Today, high quality threat intelligence is paramount, as it is the key means of responding and providing defendable computing services. Efforts are necessary, not only to obtain actionable intelligence, but also to process it, match it with traceability information such as network traffic and service logs, and to manage the findings appropriately. In order to achieve this, the community needs to take a three-fold approach: exploit its well-established international collaboration network; participate in vetted trust groups; further liaise with the private sector and law enforcement.

Tertiary Keyword (Optional)

Network systems and solutions

Primary Keyword (Mandatory)

Security and policies

Secondary Keyword (Optional)

Computing models

Author: WARTEL, Romain (CERN)

Presenter: WARTEL, Romain (CERN)

Session Classification: Track 8: Security, Policy and Outreach

Track Classification: Track 8: Security, Policy and Outreach