Contribution ID: **62** Type: **Oral Presentation**

A distributed network intrusion detection system for large science facilities in IHEP

Wednesday, 26 August 2020 17:00 (30 minutes)

The Institute of high energy physics is operating and launching many large science facilities in China, such as BEPCII in Beijing, CSNS in Guangdong and JUNO in Shenzhen. These large science facilities are facing many network security threats. How to detect and prevent these threats is becoming important.

Considering that the network traffic of large science facilities has obvious characteristics and the timeliness of different network attacks, a centralized traffic storage and distributed intrusion detection system is considered. The main task of the distributed part is to obtain data and detect real-time threats that can immediately affect the network. This part is considered to use the distributed probes, the probes are responsible for collecting and light-processing data and transmitting them to the central platform, and are also responsible for the anomaly detection of these data, screening out the abnormal parts, such as DoS attacks, then marking and transmitting them to the central platform for comprehensive analysis. The central part is the central storage and analysis platform, which is used to receive, store and mine the data.

The central part is the central storage and analysis platform, which is used to receive , store and mining the data.The design of the system framework has been finished currently and the machine learning technology is to considered to do the data analysis in the future.

Primary authors: Mr QI, Fazhi (Institute of High Energy Physics,CAS); Dr YAN, Tian (IHEP); LIANG, Zhongtian (IHEP)

Presenter: LIANG, Zhongtian (IHEP)

Session Classification: Network, Security, Infrastructure & Operations Session

Track Classification: Network, Security, Infrastructure & Operations