Contribution ID: **23** Type: **not specified**

Status of Network Security Operations at IHEP

Tuesday, 7 March 2017 17:00 (30 minutes)

Institute of High Energy Physics (IHEP) is an institute of Chinese Academy of Sciences which explore elementary particle physics. The network of IHEP campus and data center connects about 1200 servers and 3000 PC clients. It supports IPv4 and IPv6 protocols, both of them has 10 Gbps internet access.

This report gives a brief introduction to the status of network security operations at IHEP. Firstly, an architecture overview is presented. Then four subsystems are described in detail, including a monitoring and early warning system, an intranet proactive defense system based on user behavior, a network security self-service platform and a cyber-security federation for HEP community in China.

A network security monitoring and early warning system was developed and deployed based on a 10 Gbps network probe. By monitoring the network traffic data and analyzing the log of network devices and servers, it can find out the malicious IP addresses and then block the attack by associated firewall. The affected hosts in local network can be located too. A warning system is integrated and it will send short messages to administrators when high risk attack appears.

An intranet proactive defense system was designed as a supplement of traditional strategy of network boundary protection. It's based on user behavior analysis with help of artificial neural network. Suspicious user behavior can be detected and visualized, as well as early warning and even proactive attack block.

In order to help users getting rid of their host vulnerability, we developed and deployed a network security self-service platform. This system can present straightforward result of quantized fuzzy evaluation of host security risk. The result is obtained by analytic hierarchy process and cloud model theory. We improved the multi-level index system of the analytic process by dynamic weight method, which increased the adaptability and objectivity of the index system.

In June 2016, we proposed a China cyber-security federation for high energy physics (CSFHEP), about 10 universities and institutes have joined in this federation. The constitution of CSFHEP is completed and the federation is now in test run. In framework of CSFHEP, a cooperative security response center and a cyber-security study group are founded. All the members will benefit from this federation on security incident response support, threat information sharing, training on secure operations and other related services.

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

Co-authors: Prof. AN, Dehai (Institute of High Energy Physics, CAS, China); Prof. MA, Lanxin (Institute of High Energy Physics, CAS, China)

Presenter: Dr YAN, Tian (Institute of High Energy Physics, CAS, China)

Session Classification: Network, Security, Infrastructure & Operations II

Track Classification: Networking, Security, Infrastructure & Operations