Understand your network

Security Visualization usually shows a large variety of abstract data. AnNetTe makes important features obvious.

Find attacks easily

The clear interaction pipeline creates insight for every user. No large disk space or high performance is required.

Summarize events

By individualizing the complex information, you can create a clear fingerprint of suspicious network events.

Visual Analytics Pipeline

User Interaction

- select time
- select anomaly

Visualization

- Timeline
- IP Ring
- Connection River

- explore
- exclude IPs
- select IPs

- explore
- exclude connections
- find result

Network Security Event

Case Study

DoS Attack

- Attack Feature
  - Low destination IP Entropy
  - High source port entropy
  - Low destination port entropy
  - Dominating suspicious connections
  - Large amount of connections

- Event Description
  - IPs 10.6.6.6, 10.6.6.13, 10.6.6.14, 10.7.6.3, 10.7.7.10, 10.11.6.15 and 10.100.1.6 use many ports attacking port 80 of the http server 172.30.0.4.

Network Scan

- Attack Feature
  - Low destination IP Entropy
  - High destination port entropy
  - Dominating suspicious connections
  - IPS warning of access deny
  - Suspicious IP attacks multiple times

- Event Description
  - IPs 10.10.11.15, 10.9.81.5 scan large range of ports of all http servers in the subnet of 172.20.0 and 172.10.0. Health status of servers are not good.

Acknowledgements

This work is supported by National NSFC Project (No. 61170204) and National NSFC Key Project (No. 61232012). We thank domain expert Zhuo Zhang from QIHU Co. for his valuable suggestions and feedback. We thank H. Bosch, S. Koch, R. Krueger and D. Thom for their comments. Hanna is supported by Baden-Wuerttemberg Stiftung for participating in this collaboration.