CINBAD keeps an eye on the CERN network infrastructure

Ryszard Erazm Jurga, Milosz Marian Hulboj
CERN, Geneva, Switzerland
Ryszard.Jurga@cern.ch

Abstract. The CINBAD (CERN Investigation of Network Behaviour and Anomaly Detection) project was launched in 2007 as a collaboration between CERN and HP ProCurve Networking. The project’s aim was to understand the behaviour of large computer networks in the context of high performance computing and large campus installations such as at CERN. The specific goals of the project were to be able to detect traffic anomalies in such systems, perform trend analysis, automatically take counter measures and provide post-mortem analysis facilities. This paper will present the background, data sources, data collection and analysis approaches as well as the findings.

1. Introduction
In the old shared Ethernet, network engineers, security administrators, service managers, application developers and other network users could see all the traffic from any place in the network using, for instance, the tcpdump tool. Whether or not it was appropriate, this was surely a very useful facility to debug applications, investigate network problems as well as detect anomalies. This possibility disappeared with the arrival of switched networks which deprived users of full traffic monitoring. The CINBAD project [1] brings a similar functionality back for authorized users.

2. Network infrastructure challenges
Contemporary networks are becoming more complex and difficult to comprehend and manage. A typical network comprises many different elements like switches, routers, servers, and user machines - along with a myriad of services and applications. CERN's campus network has more than 50,000 active user devices interconnected by more than 2500 switches and routers and 10,000 km of cables and fibres. The potential 4.8 Tbps throughput within the CERN network core and 140 Gbps connectivity to external networks offers countless possibilities to different network applications. At the same time, the number and scale of potential network problems, attacks and viruses will almost surely increase. Network security is becoming increasingly important for all types of business, as any disruption can result in losses (profit, customers, company image, etc). This fact, combined with the CERN specific configuration and topology, makes network behaviour analysis a very challenging but important task.

3. CINBAD project principle
The CINBAD project collects and stores data from various parts of the CERN network, including the network configuration database, server logs, user reports, network traffic as well as other monitoring systems. This data is then made available for correlation by means of CINBAD applications. Its diversity allows us to look at the network from different perspectives. This provides potential users of the system with more accurate information about the status of the CERN network and more reliable
detection of anomalies. However, the most interesting information is probably buried in the packets from network traffic – the principal CINBAD data source.

4. Sniffing the network infrastructure
With modern high-speed networks it is impossible to monitor all the packets traversing the links. Currently, detailed analysis of the network traffic is only performed at critical points on the network (firewall and gateways between network domains). This might require significant computing power to collect and analyse the traffic and still does not guarantee correct results, particularly in the anomaly detection domain (as the anomalies might be local and not propagate beyond the critical points). However, CINBAD overcomes this issue by using only the sample traffic and statistical analysis. sFlow [2], a technology for monitoring high-speed switched networks, provides randomly sampled packets from the network traffic from almost all the links at CERN. In fact, sFlow is derived from a collaboration between HP, the University of Geneva and CERN in 1991. It is based on packet sampling [3] where on average 1-out-of-N packets is sampled by an agent and sent to a collector. This sampled data consists of the initial 128 bytes of an Ethernet frame and contains switching/routing/transport protocol information, part of the application protocol data (e.g. HTTP, DNS) and is complemented by a set of SNMP counters. Low CPU/memory requirements make switch implementation of sFlow agents scalable and suitable for large network infrastructures. For a large computer network such as CERN’s, this sampled traffic contains much statistically-interesting data which serves as the basis for analysis.

5. Collecting and storing network traffic
Sampled traffic is being collected from approximately 1000 switches in the CERN network by a multi-stage sFlow collector that has been up-and-running for more than two years. At the first stage, every five minutes sFlow tree-like format datagrams are unpacked and stored in CINBAD file format, compatible with the pcap library. This enables a fast direct access by means of a wide range of tools (e.g. tcpdump, wireshark or snort – see 7.1). In addition, data is complemented by metadata information about the origin of sampled packets, which in total represents approximately 3 TB of data stored per month. In order to reduce the storage space and to draw meaningful conclusions about the network traffic, this data is further aggregated and stored in a database. The following key packet attributes are preserved together with their numbers of occurrences and sizes:

- Device and interface where a packet was sampled
- Source and destination MAC/IP addresses
- Protocol type
- Source and destination TCP/UPD ports
- Protocol specific information (e.g. TCP flags, ICMP codes)

For each five-minute time interval and for a unique combination of these attributes, a database entry is added to one or more tables. These entries are then used by a variety of tools in order to monitor the CERN network infrastructure as well as to detect anomalies.

6. Seeing through and beyond the CERN network infrastructure
The CINBAD-eye (C-eye) tool suite has been developed to simplify the operation and problem diagnosis process in the CERN network as well as to understand the network evolution and provide valuable information for future designs.

C-eye provides detailed port statistics about the traffic sent and received by all monitored switches. The information is available for any given time interval with five-minute resolution and consists of sFlow, SNMP counters and the distribution of traffic protocols. This basic piece of information, complemented by the network configuration database, is of interest for network operations as it provides evidence of active connectivity behind monitored ports. Further traffic details such as MAC
and IP addresses enable operators to identify a machine connected to a given port as well as to validate the consistency between the desired and actual state of IP and MAC address mapping. In addition, C-eye provides details about sampled traffic flows associated with a given machine, including information on where these flows have been seen in the network. This provides valuable input for an understanding of the current network behaviour and facilitates inference about the nature of the traffic from all machines.

The above information is also useful for network design and provisioning. Periodic database jobs compute various daily statistics. The details include the amount of data collected from the network, average protocol distribution, sampling ratios, average number of machines connected to a switch port, and the number of traffic flows in respect to internal and external traffic. The C-eye tool enables users to observe changes in this information for long time intervals and conduct their analysis either on the whole network or on specific parts, like the wireless network, individual buildings or switches. This functionality helps to understand the network evolution and provides valuable input for the future design. In addition, this quantitative information could be compared with the service-level agreements specified for network usage.

C-eye also provides a front-end interface (also known as CERN-wide tcpdump) to access files with collected packets. This functionally enables advanced users to filter packets out by means of three filters: pcap filter, sFlow filter as well as by a regular expression. The result is saved in pcap format and can be analyzed by any tool that reads pcap files. This is particularly useful for investigations where aggregated information does not provide enough details and where access to packet payload is desirable.

Other C-eye suite tools benefit from the analysis of application data in sampled packets and provide information about the inventory of various services at CERN, dissect Domain Name System (DNS) requests, etc. The findings are used to complement data obtained from other monitoring systems. This enables detecting both official and non-official network services, wireless access points and areas with high IP roaming rates. This application data also helped to detect machines infected by the Conficker worm by identifying malicious DNS lookups.

With all of these functionalities, C-eye offers a comprehensive toolkit to facilitate day-to-day network operations, diagnose network problems, perform post-mortem analysis and provides an insight as to how the future of the CERN network might look like.

Figure 1. CINBAD-eye

7. Detecting known and unknown security threats
Detection of security threats in the network was another area explored by the CINBAD project. While one could find many interesting papers on this topic, at the time when the project started there were very few publications on sample-based analysis. Most of the approaches required either full data or special hardware support to perform deep packet inspection. In contrast, CINBAD anomaly detection is based on two independent approaches: statistical and signature-based analysis. The former depends
on detecting deviations from normal network behaviour, while the latter uses existing problem signatures and matches them against the current state of the network.

The synergy between these two approaches provides the detection system with a fast and reliable detection rate that is also able to detect the unknown anomalies and to produce new signatures.

**Figure 2. CINBAD anomaly detection system**

### 7.1. Detection of known anomalies

The signature-based approach is based on an insight into the payloads of packets provided by sFlow and SNORT (an open-source intrusion-detection system). SNORT has been ported to work with sampled data. This included changes in the SNORT source code related to truncated packets’ payloads as well as the translation of stateful SNORT rules into stateless ones. In addition, the SNORT application has been wrapped by the tool which automatically reads newly collected data, and periodically updates rules from projects like Emerging Threads. Snorts’ alerts are logged into a file as well as into a database. This system has been operational for more than two years and detected a certain number of anomalies in the CERN network. It appears that most of them originated from end-user machines and were related to various viruses, worms and usage of prohibited applications at CERN (e.g. P2P file sharing, IRC instant messaging, Tor).

### 7.2. Detection of unknown anomalies

Even though the signature-based approach seems to perform well and generates few false-positives, the system is blind and can yield false negatives in cases of unknown anomalies. In order to overcome this limitation, the statistical analysis based on the multivariate analysis technique is applied.

The principle of this technique is based on building and continuously updating various network profiles. Once these normal profiles are well established, the statistical approach can detect deviations from the ‘normal baseline’ and detect new and unknown anomalies.

The selection of robust metrics that are resistant to data randomness plays an important role in characterizing the expected network behaviour. The number of metrics can vary significantly and depends on the target for which the profile is built (e.g. whole network, sub-network, host, protocol). Potentially, this number can be very high [4], since one feature might be either a linear or non-linear combination of the others. After investigations and experiments performed on data sets with various anomalies, the following four basic metrics have been indentified:

- number of distinct destination addresses contacted by the host
- number of distinct destination ports contacted by the host
• average number of destination ports per destination address contacted by the host
• average number of destination addresses per destination port contacted by the host

In addition, collected data is clustered into internal and external traffic, further divided into three protocols groups: TCP, UDP and ICMP and finally into several classes according to TCP/UDP port numbers. This clustering also implies an adjustment of the basic metrics and includes more protocol specific features. For example, for the TCP protocol it is reasonable to narrow the analysis to certain packet types e.g. TCP/SYN packets, otherwise the obtained results are very noisy because of dynamic and private TCP ports.

For all sub-groups the network status matrices are built every five minutes with a number of columns related to the basic metrics above, and with a number of rows equal to active CERN hosts. Every five minutes the distances between new matrices and their baselines are calculated. For this purpose, entropy is calculated for every column (metrics). In the next step, a distance is calculated between current and baseline entropy vectors and results from this calculation are used to build time series.

In order to mitigate the noise that can arise from calculating distance between two matrices the weighted moving average smoothing function over a few five-minute long time intervals is used to calculate baseline values for all hosts. Hosts that do not appear for longer time intervals are removed from the calculation.

The usage of entropy for anomaly detection is a quite new approach but there is a common belief that detection methods based on entropy are more resilient to sampling than others [5]. There are already a few examples showing entropy and its practical applications in anomaly detection in networks [6, 7, 8] and in Space Shuttle Main Engines [9].

For around 10,000 hosts with random distribution of metrics values, entropy is approximately equal to 1. If there are one or a few hosts that stand out from others, the entropy value will drop. Such a drop will be interpreted as an anomaly if it falls below a threshold. Since the network environment is very dynamic, the weighted moving averages and the moving variances are used to build a moving threshold and to reflect network dynamics. In order to mitigate the impact of the anomaly on the average and variance, the anomalous data points are not taken into account for the next time intervals.

![Figure 3. CINBAD statistical-based anomaly detection](image)

7.3. From unknown to known anomalies
Anomalies that were detected by the statistical-based approach but went undetected by the SNORT engine are further analyzed manually. If this is possible, a signature is generated by means of a supporting tool and it is then fed back to the SNORT engine. This tool uses SeqAn’s [10] implementation of the Longest Common Subsequences algorithm. However, this approach to produce signatures is heavyweight and cannot be used efficiently on huge sets of packets. For this reason, the tool is only fed with data relevant for a detected anomaly. Using this approach we have identified signatures that were mostly related to P2P and instant messaging applications.

8. Conclusions

CINBAD has proved to be a very interesting and fruitful collaboration between CERN and HP ProCurve Networking. The CINBAD project was able to deliver high quality tools for network monitoring, troubleshooting, forecasting and anomaly detection that are being used at CERN. We have shown that it is possible to obtain global network visibility on high-speed links with the robust packet sampling offered by sFlow. Together with the network engineers at HP we have created an application to facilitate day-to-day operations by providing detailed information about the status of the network at any point in time. CINBAD has also demonstrated the possibility of distributed anomaly detection at the edge of the network with sampled data.

References
[1] CERN openlab CINBAD project webpage http://cern.ch/openlab-cinbad
[2] The sFlow webpage http://www.sflow.org
[3] P. Phaal, S. Panchen, N. McKee, “InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks”, 2001
[4] F. Wanner, “Anomaly analysis using host-behavior clustering”, ETH – Swiss Federal Institute of Technology Zurich, 2007
[5] D. Brauckhoff, B. Tellenbach, A. M. May, A. Lakhina,”Impact of packet sampling on anomaly detection metrics”, Proceedings of the Internet Measurement Conference, 2006.
[6] A. Wagner, B. Plattner “Entropy based worm and anomaly detection in fast IP networks”, Proceedings of the WETICE conference, 2005
[7] A. Lakhina, M. Crovella, C. Diot, “Mining anomalies using traffic distributions. Technical Report 2005-002 CS Department, Boston University”, 2005
[8] G. Nychis, “An empirical evaluation of entropy-based anomaly detection”, Information Networking Institute Carnegie Mellon University Pittsburgh, PA 15213, 2007
[9] K.Tumer, A. Agogino, “Entropy based anomaly detection applied to space shuttle main Engines”, Proceedings of the IEEE Aerospace Conference, 2006.
[10] The SeqAn webpage: http://www.seqan.de