Internet Measurements and Analysis Workshop 5 April 2023

When: Wednesday 5 april 2023

Where: SURF Utrecht Room 3.5

Please register: here

Agenda

10:30	11:00	arrival		
11:00	11:30	Understanding inter-domain routing in our current Internet has become significantly more complex over the last decade. The volume of both BGP speakers and their announcements has increased, but moreover, deployment of RPKI Route Origin Validation leaves operators with a less transparent view on parts of their networks and equipment. With Rotonda, the Routing team at NLnet Labs aims to provide operators and researchers a modern, modular software stack focusing on collection and analysis of real-time routing data. The BGP Monitoring Protocol (BMP) is the principal way of getting data from routers into Rotonda. We go into the basic concepts of BMP, its pros and cons compared to other ways of collecting data, and touch upon how recent developments of the protocol can further help with routing observability.	Luuk Hendriks (NLnet Labs) Jasper den Hertog (NLnet Labs)	slides
11:30	11:50	In this talk I will share some details on our usage of BMP in the SURF network. For our SURFinternet service we have a lot of peering sessions with external networks. To get some insights in what is happening in these peering sessions, we started looking for a robust monitoring setup that is more feature-rich then just SNMP traps. Since this is very much a work in progress, I wil share some details on what tools we looked at and what we use today, some examples of events where BMP gave us a clear advantage in pinpointing an issue and to close the talk, I'll give some sneak peeks on what we plan to do with all the data we gather.	Joachim Opdenakker (SURF)	slides
11:50	12:10	Society's dependence on the internet has grown over the years: The internet changed from being just a network of networks to the foundation of many social and economical transactions. This change poses new challenges in the areas of transparency, responsibility, and sustainability that were never considered in the early years of the Internet. Transparency forms the foundation for internet responsibility and sustainability. Especially when multiple intermediate networks need to be traversed while transporting data, networks need to be transparent about the manner the data is processed or how much energy is consumed during the transport of the data. Only with the right information a user can make intelligent decisions about how their data will be transported. To provide transparency on the existing internet, we earlier developed a tool named PathVis to provide users with insights on how their network traffic traverses to its destination. With PathVis, we attempted to combine selected information from existing sources into a view of how one connects to the Internet. We knew beforehand that there are a multitude of information sources of different quality levels available but combining the information from these sources into something reliable and usable is not trivial. To improve the quality of information about independent networks, we propose an Autonomous System Information Service (ASIS): a self-hosted approach for sharing interoperability and policy information of a communication network. The ASIS gives a network (Autonomous System or AS) the autonomy to decide whether to run such a service or not and what information they share with whom. We believe the ASIS can contribute solve some of the aforementioned challenges by facilitating internet transparency.	Caspar Schutijser (SIDN Labs)	slides

12:10	12:30	Recently, there has been growing interest in offloading NFs to programmable network devices. Unfortunately, it is currently not possible to maintain the full state of NFs during a switch reconfiguration without consuming network resources from and to neighboring switches. We present State4, a framework that maintains the state of P4 programs during the reconfiguration of a programmable device, by only using a small number of local resources on the switch undergoing reconfiguration. State4 acts on both the in-switch control-plane and the data-plane. By utilizing the in-switch local controller, State4 requires no external network resources to achieve stateful reconfiguration. As such, State4 enables on-the-fly reconfiguration of stateful NFs, at minimal traffic disruption, where previously traffic had to be re-routed.	Chenxing Ji (TU Delft)	slides
12:30	14:00	lunch		
14:00	14:30	In this presentation we look at changes in the Internet in Ukraine since the start of the war as can be seen from RIPE RIS and RIPE Atlas.	Emile Aben (RIPE NCC)	slides
14:30	15:00	The ultimate objective of the programmable networking research by TNO is to create a self-optimizing network service infrastructure, based on open networking and cloud technology. In this research project we make a step towards this long-term objective by investigating state-of-the-art the programmable network telemetry and its application to monitor and optimize end-to-end performance of advanced network services. Specifically, the objective is to create a system to collect and integrate telemetry data from the network, from the cloud systems hosting applications and – if possible – from the applications themselves. As a specific use case for applying programmable end-to-end performance telemetry, we select eXtended Reality (XR) services. XR services are known to be highly demanding both from network (e.g., high bandwidth demand, low jitter) and processing perspective (e.g., transcoding latency). In our talk we will discuss the architecture of the eXtended Reality system, developed in TNO SocialXR programma, instrumented in this project with various telemetry functions. We will touch upon network, cloud and application monitoring. We will present both successful developments as well as the difficulties that required workarounds or even problems that we could not solve. Finally, we will mention on how collected telemetry data is envisioned to be linked to the XR Quality of Experience.	Piotr Zuraniewski (TNO)	slides
15:00	15:30	break		
15:30	16:00	We've been developing a flow-based, lightweight network traffic capture retention recommendation system. At a very high level, it is a system that ingests flow data (IPFIX or Netflow v9), applies lightweight math, and issues a binary recommendation (keep/discard) that indicates that a capture window is suspect or not (e.g., DDoS or spoofing activity). The underlying idea is that it'll allow network operators of non-backbone networks to continuously capture full network traffic payload in tumbling windows (e.g., 5min) and, next to aggregate flow data, only keep captures that the recommendation system indicates may be needed for forensic purposes later on.	Mattijs Jonker (UTwente)	slides
16:00	16:30	Commercial Virtual Private Network (VPN) providers have steadily increased their presence in Internet culture. Their most advertised use cases are preserving the user's privacy, or circumventing censorship. However, a number of VPN providers nowadays have added what they call a streaming unblocking service. In practice, such VPN providers allow their users to access streaming content that Video-on-Demand (VOD) providers do not provide in a specific geographical region. In this work, we investigate the mechanisms by which commercial VPN providers facilitate access to geo-restricted content, de-facto bypassing VPN-detection countermeasures by VOD providers (blocklists). We actively measure the geo-unblocking capabilities of 6 commercial VPN providers in 4 different geographical regions during two measurements periods of 7 and 4 months respectively. Our results identify two methods to circumvent the geo-restriction mechanisms. These methods consist of: (1) specialized ISPs/hosting providers which do not appear on the blocklists used by content providers to geo-restrict content and (2) the use of residential proxies, which due to their nature also do not appear in those blocklists. Our analysis shows that the ecosystem of the geo-unblocking VPN providers is highly dynamic, adapting their chosen geo-unblocking mechanisms not only over time, but also according to different geographical regions.	Etienne Khan (Utwente)	slides

16:30	17:00	Resource Public Key Infrastructure (RPKI) and Route Origin Validation (ROV) adoption has increased significantly over the last couple of years. However, as we have recently seen, not every network that does ROV has the same impact on where traffic goes – for example if it is surrounded by networks that do not do ROV. With this research we want to find out whether we can find out which networks do not do ROV yet, and whether we can rank them based on the impact they would have on the global internet if they did do ROV. We do this by announcing a valid less specific prefix from an anycast network, and a more specific invalid announcement from one location. We use RIPE Atlas and the NLNOG Ring to then perform traceroutes to two addresses: one that is inside the less specific and inside the more specific, and one that is inside the less specific and not inside the more specific. We then compare at which hop and Autonomous System (AS) the traffic deviates, and analyze which ASes are most prevalent.	Kevin Klercq (UvA SNE) Koen van Hove (NLnet Labs) Willem Toorop (NLnet Labs)	slides
17:00		drinks		