APNIC56: "Technical 1"

Florian Suess

12th September 2023

Summary

The "Technical 1" session comprised of four speakers.

- Yurie Ito - Founder and Executive Director of CyberGreen Institute
- Binh Lam - Director, Engineering and Operations at NTT Australia
- Edward Lewis - Senior Technologist at ICANN
- Shishio Tsuchiya - Systems Engineering Lead at Arista Network

Respective Themes

I couldn't find a way to broadly summarise these speakers topics without using unhelpfully broad language; so here is a respective breakdown of the talks given.

Idea: "Cyber Public Health"

Yurie comes in with an introduction to the concept of "Cyber Public Health", drawing parallels between public health and cyber security. She pitched the need of understanding underlying risks and adopting data-driven strategies similar to public health approaches to enhance cyber security on a per country basis. Highlighting a project called Internet Infrastructure Health Metrics Framework (IIHMF) to measure internet infrastructure health interestingly aimed to guide policy makers in evaluating cyber risks and policies.

Observation: "Vulnerable Ports"

Binh, dives into cybersecurity with a focus on internet protocols, ports, and their associated threats. He emphasizes the dangers posed by commonly used, outdated ports and protocols, sharing personal experiences and observations. He demonstrates a tool, shodan.io, for auditing network infrastructure to identify vulnerabilities. He recommends a proactive approach, such as utilizing "Access Control Lists", disabling unnecessary services, and patching known vulnerabilities to enhance network security.

Observation: "Adoption of ROA and DNSSEC"

Edward, explores the intersection of domain name systems and routing systems, with a particular focus on route origin authorization (ROA) and domain name system security extensions (DNSSEC). Focusing on the adoption rates of ROA and DNSSEC rather than the ideas themselves, expressing concern over the current low adoption rates. He also touches on the lack of IPv6 deployment in some top level domains (TLDs). He urges a deeper understanding of operators' reluctance to adopt these security measures, advocating for a dialogue to make security enhancements more operator-friendly.

Demonstration: "EVPN protocol"

Shishio discussed EVPN (Ethernet VPN) multihoming and high availability networking, reflecting on its merits and technical design points. Detailed the protocol's capabilities in ensuring network reliability and handling traffic in different network topologies. They also touched on how EVPN supports

multi-vendor environments, enhancing interoperability. The speaker emphasized the importance of open standard technology for improving network availability to benefit consumers, businesses, and IoT services, and concluded by encouraging the adoption of EVPN multi-homing technology for high availability networking.

My Key Insights

"Cyber public health" is something that I had never thought of before; that is effectively setting KPI's that could drive policymakers.

Most impactful were the two observation talks though. The coverage on open vulnerable ports discussion was very easily followable, with amazingly rich diagram showing the process of an attack well known as the "AWS Route53 BGP hijack" and the detailed per port explanation of vulnerabilities - necessitating the refresh of commonly known reserved ports in general. Counter-intuitively (as I will explain in the assessment section below) I found Edward's talk most helpful due to the lack of definitions re: ROA and DNSSEC or the idea's behind them and the subsequent high cadence of relevant abbreviations. This motivated quite a bit of study just to keep up triggering a very meaningful deep dive into the implementation details of ROA and DNSSEC, topics I never really looked into before.

Assessment

As mentioned, the high use of jargon, especially in Edward's talk about ROA and DNSSEC adoption, might have alienated individuals new to the field (I barely kept up, and I come from a decent background). A glossary or a brief explanation of terms could have bridged this knowledge gap, creating a more inclusive learning environment.

On the contrary, Binh's segment on open ports was well-articulated and easy to digest, catering to a broader audience spectrum.

The format provided lacked in the ability to provide a slower pace, and deeper dive into some topics discussed as part of the EVPN talk... The session could have also been enhanced by a more interactive format, the attempt to integrate a Q&A segment after each presentation to address any queries or confusions in real-time was too compressed in practice and led to it being cut.

Having written this assessment in hindsight, Eward's talk in particular was much better suited to be paired with "Technical 3"'s "RoVista framework" talk due to the very big domain overlap.

APNIC56: "Technical 2"

Florian Suess

12th September 2023

Summary

The "Technical 2" session comprised of three speakers.

- Ulrich Speidel - My CS742 Lecturer
- Takashi Tomine - Research Engineer at the NAOJ
- Geoff Huston - Chief Scientist at APNIC

Respective Themes

Again, hard to surface key themes in the discussed topics, although Ulrich and Geoff had a tiny bit of overlap when it came to performance measuring Starlink (although in very separate contexts).

Observation: "Starlink offering"

Provides experience and findings with SpaceX's Starlink service, emphasizing its benefits, challenges, and potential. Ulrich touched on Starlink's fast evolution, better performance over geostationary and medium earth orbit connections, cost-effectiveness, and its transformative impact on regions with no internet access. Highlighted that despite the rapid growth, Starlink is experiencing growing pains, and it's unlikely to connect the 2.7 billion disconnected or underserved individuals globally anytime soon due to capacity and regulatory challenges that set it behind as clarified in the Q&A by up to two orders of magnitude. The discussion also involved technical aspects like satellite tracking, latency, and potential mobile service. Audience queries involved capacity, satellite replacement timelines, and connectivity types, explaining that the current primary service is from Starlink infrastructure to the user, with some potential for point-to-point links on the ground via Starlink, albeit not mature yet.

Promotion: "Interop Tokyo ShowNet"

Beginning with the motivation behind the importance of interoperability in internet technologies, underlining how it's crucial for the extension and functionality of the internet. The speaker references an event "InterOp Tokyo", an annual exhibition in Japan that showcases the latest in internet technologies and provides a platform for interoperability testing, emphasizing on its long history since 1994. They touch on the ShowNet project, a large-scale demonstration network set up at InterOp Tokyo, which provides a unique environment for interoperability testing among multiple vendors and the visitors can witness new technologies or protocols running in a mixed environment. They delve into various technical challenges and solutions explored over the years, mentioning specific technologies like SRv6, EVPN, DWDM, and RPKI. The speaker emphasizes the importance of such real-world testing environments in advancing internet technologies and mentions their intent to continue these efforts to foster the progression of internet technology.

Opinion: "QUIC vs. TCP"

Discussing the evolution and limitations of TCP, emphasizing the transition to QUIC (Quick UDP Internet Connections) due to its benefits in encryption, congestion control, and speed. He showcases how major platforms like Google and Facebook have

adopted QUIC for better performance and encryption, enabling them to retain control over user data for competitive reasons. Points out how QUIC's rise signifies a shift of value and control towards the application layer wrt. the OSI model, leaving the network layer as a valueless commodity. This shift, he predicts, will define the industry's next decade, pushing the traditional networking models to the background while applications take the forefront in driving technological advancements.

My Key Insights

The two notable talks for me was the Starlink and QUIC migration observations - both talks similarly where based on topics I was aware of but hadn't looked into deeply. I honestly saw Starlink more as an early stage concept rather than a real tool that has significant usage. Notably I enjoyed the section around the evidence indicating the use of heuristic based classifications of geographical areas based on existing connections as opposed to known urban vs. rural. The coincidental highlighting of the benefit's of non-geostationary satellites (Q&A highlighted) wrt. to system redundancy and more. The frank language employed presentation by Geoff was a fun listen - the interesting insights to "local data traffic" as opposed to long-haul traffic led to an interesting conclusion of his re: routing security hence being an outdated topic. Most interesting in this talk though was highlighting of the shift of value and control towards the application layer, leaving the network layer as a valueless commodity. Showcased that this shift is more heavily motivated than the contrasted IPv6 migration, as it leaves for a stronger incentive for competing technology giants by placing "data control" on a pedestal.

Assessment

As opposed to "Technical 1", the Q&A facilitation was certainly better and richer which made this session a lot more interactive in my eyes, although in the right direction, I would've liked to seen even more. Particularly good questions asked especially to Ulrich's session. One observation that caught my attention was the assertion that routing is becoming less pivotal in the context of localized traffic. Although this was an intriguing proposition, it felt slightly underexplored. There was potential for a wider discourse, especially considering how audacious such a statement is in the contemporary networking landscape. This sentiment also applies to the bold declaration that "TCP is dead." While this may have been a strategic exaggeration to spark interest, it would have been enriching to see this topic explored further in subsequent discussions. I noticed that some of the adjacent talks, even if they weren't directly related to this session, seemed to place TCP at the heart of their assumptions. This dichotomy warranted more attention. I really appreciated the publicity given to "Interop Tokyo ShowNet" project, it's such a good place for this advertisement and was motivated in a really good way (importance interoperability). Ofcourse, we must point out that the level of verbal English exercised was tricky to follow in this talk.

APNIC56: "Technical 3"

Florian Suess

12th September 2023

Summary

The "Technical 3" session comprised of only two speakers! This allows us to go into more depth than previous summaries on a per talk basis.

- Tijay Chung - Assistant Lecturer at Virginia Tech
- Azhar H Khuwaja - Community Trainer

Demonstration: "RoVista Framework"

As a preliminary; Resource Public Key Infrastructure (RPKI) and Route Origin Validation (ROV) is covered. In a sense, these are security frameworks that are designed to secure the Border Gateway Protocol (BGP), which is the routing protocol used on the internet. RPKI is used to validate the authenticity of route announcements made by systems on the internet (IP holders, like ISP's) and then ROV is the process of using RPKI data to validate BGP route announcements. This authenticity framework prevents BGP route hijacking (related case study on a compromise would be the "AWS's Route 53 hijacking"). Ofcourse this isn't inherent, one must explicitly adopt this. TiJay showcases some tools, such as Cloudflare's hosted tool, "is bgp safe yet" that allows for the testing of your ISP's compliance.

TJ explains the RoVista framework's utility in understanding and measuring the ROV status of network operators, with a focus on securing internet routing structures using RPKI. Tijay detailed the current deployment status of RPKI, challenges in tracking its implementation, and how the RoVista methodology uses techniques like internet protocol identifier (IPID) side channel to detect ROV policies; determining if certain traffic (specifically, traffic from IP addresses flagged as invalid by RPKI) is correctly being filtered between hosts. He shared RoVista's measurement findings and noted its limitations. TiJay concluded by announcing the upcoming academic paper on the topic and encouraged network operators to join their survey for more comprehensive data collection.

Observation: "Adoption of OAM"

This talk delved into Carrier Ethernet OAM (Operations, Administration, and Maintenance), emphasizing its decade-long commercial availability yet noting its less-than-expected adoption. He highlighted the two predominate standards "802.1ag" and it's extension "Y.1731" in guiding Carrier Ethernet operations and described tools to monitor and ensure Service Level Agreement's (SLA) compliance. He noted that these standards as opposed to others in the same housing suite is non-intrusive (hence de-motivating any reasoning due to service impact upon adoption). Azhar continues by discussing key metrics like delay, jitter (termed "inter frame delay variation" in Ethernet), frame loss ratio, and availability. Ofcourse it wasn't difficult to understand the concluding remarks on the significance of exporting these metrics to Network Management Systems for effective visualization and assessment.

My Key Insights

Although this session was the shortest of the three "technical" sessions today, this one was the most challenging to follow. The first session on 'IPID side

channel' showcased an approach in detecting ROV policies (more interesting to others that can readily contrast this approach to existing). The explanations provided offered me a re-affirmation of the needed perspective on the vulnerabilities inherent even within systems that are often just assume secure ("Technical 1" goes through the lack of ROA adoption which pairs nicely with this). The talk by Azhar was surprising, to learn that despite being commercially available for over a decade, the adoption of self monitoring standards that provides objective monitoring of SLA compliance hasn't reached its full potential (honestly a theme that tracks throughout the entire set of "Technical"'s so far). The detailed walkthrough's (that needed a lot of supplementation on my side) of standards 802.1ag and Y.1731 was particularly insightful, even how these can be neatly extended with 802.3ah. Both these sessions definitely reinforced the significance of a thorough understanding of foundational concepts/technologies in today's networking landscape.

Assessment

I really like TiJay's simplification of the problem at hand by providing the two questions in context of RPKI and ROA; "How network operators use RPKI to *claim* their IP addresses" vs. "How network operators also use RPKI to *filter* invalid BGP announcements". This simplifcation was great at motivating the RoVista framework. Azhar's talk on 'Carrier Ethernet OAM' was incredibly informative, but at times, the intricate details of the technical standards and their interplay seemed overwhelming (I had to stop frequently and just catch up). It would have been beneficial if he had occasionally zoomed out to discuss the larger picture and real-world applications.

At one point, when discussing 'inter frame delay variation,' I felt the distinction between it and the more common term 'jitter' wasn't fully explained, which could lead to confusion for those less familiar with the topic. Should probably also point out that there was also a hiccup during Azhar's session when he lost connection. Such disruptions can sometimes cause the audience to lose the thread of the topic.

Both speakers I think could have been enriched a lot with more interaction with the audience, perhaps posing rhetorical questions or hypothetical scenarios to keep engagement levels high.