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 walk-through'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.