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 He emphasizes the dangers posed by commonly used, outdated ports and protocols, sharing personal experiences and observations.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.