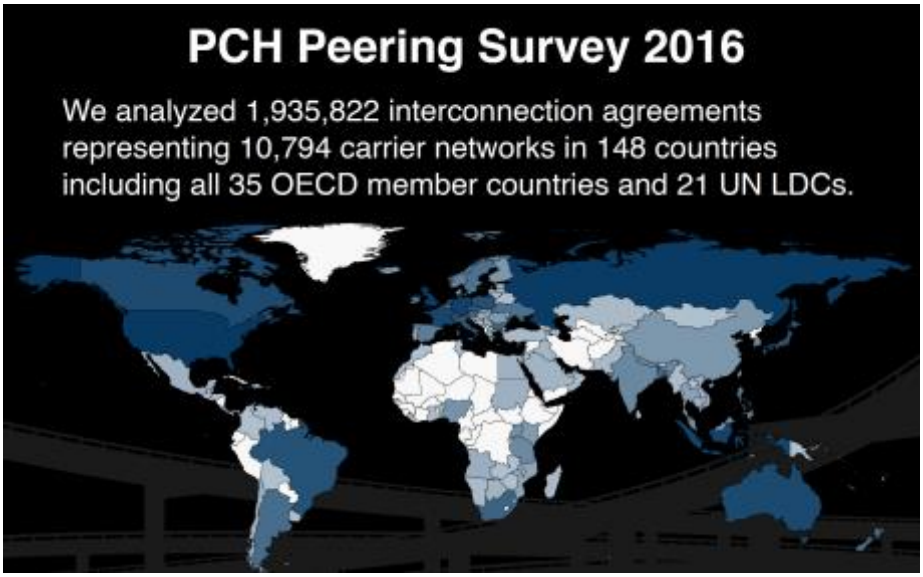
Geoff Huston
February 2017

NANOG 69

NANOG 69 was held in Washington DC in early February. Here's my notes from the meeting.

It would not be Washington without a keynote opening talk about the broader political landscape and NANOG certainly ticked this box with a talk on international politics and cyberspace. I did learn a new term, "kinetic warfare," though I'm not sure if I will ever have an opportunity to use it again! There is no doubt that the world of DDOS, abuse, cyber stuff and similar terms has a number of facets, from the technically adventurous through the merely criminal to state actors preparing both scenarios for defence and attack in the area of public communications and the Internet in particular. We used to talk about the "borderless network" but I suspect that level of naivety is long gone, and the enduring reality is that the world of politics is nasty, brutish and enduring!

The world of peering is also an area of interest to many and Bill Woodcock presented on a recent Peering Survey undertaken by PCH.



From PCH 2016 Survey of Interconnection Agreements, Bill Woodcock, Packet Clearing House

Sometimes it seems that we have replaced sandals and t-shirts in this industry with suites and ties, and the paraphernalia of marketing, products, lawyers and contracts, so I was amazed to learn that according to this study 99.93% of peering agreements between networks are based on undocumented handshakes! Equally interesting is the finding that 99.98% of peering agreements are symmetric. Given the disparity of networks in many if not all market segments, it is surprising that both parties can see an approximately equal level of benefit to undertake a peering exchange of traffic. Practically, it's not surprising to learn that nearly all peering is multi-lateral, where one party peers will all others at that exchange. Bilateral connections grow at a rate of the square of the number of players, whereas multi-lateral peering is back to a simpler O(n) scaling issue. But from a business perspective it is entirely surprising to learn that networks are opening themselves up to peer with as-yet unknown future participants in the same peering exchange. But maybe it's no longer important. Maybe every little IP

traffic actually flows from a customer edge to another customer edge, and every little of commercial significance in any rate. If you take the view that peering exchanges are changing into a "meet-me" point for handover from the Content Distribution Networks to the last mile Access Networks, as distinct from a means of interfacing between edge access networks, then the role of these accretion points of competitive access providers is useful for CDN design. The presentation did not report on any questions relating to network role (access vs CDN vs transit) or on traffic flows across the exchanges, so there is little in the way of data from this report that could either substantiate or supposition of the common role of peering exchanges these days.

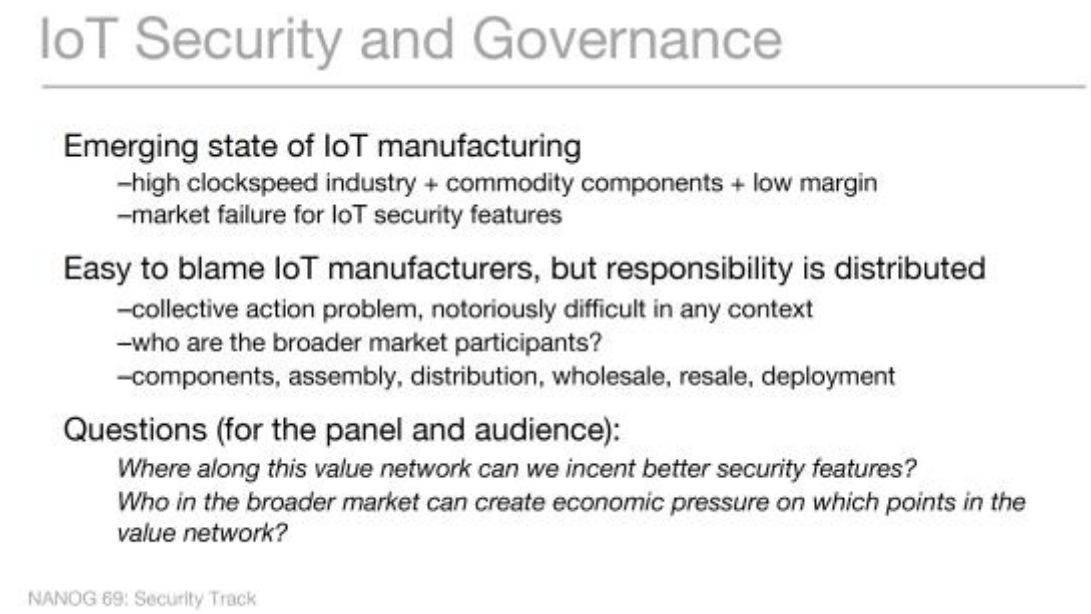
The presentation on an Internet-Wide Analysis of Traffic Policing was fascinating. The classical school of TCP rate control algorithms assumed an environment of what could loosely be described as fluid dynamics: a collection of concurrent flows sharing a common network carriage and buffer queue where each flow is attempting to roughly equilibrate its share of the common resource against those of all other concurrent flows. The common assumption is that the network is not an active intermediary here, and that a flow senses its maximum rate through the onset of buffer-occupancy derived increased latency and ultimately through packet drop. TCP's general approach of additive increase and multiplicity decrease was intended to gently exert increasing pressure on the network and on other concurrent flows over time, and back off once the network buffers were filled to the point of packet drop, and back off to a point that would hopefully allow the flow traffic stored in the buffer to drain. But if the network is actively policing traffic rates, then the onset of packet drop is immediate once the sending rate exceeds the policed level. Even when a rate limiting token bucket is being used, while the point of drop may not be fixed, the onset of drop without preceding latency variation is common in such situations. The result is that the efforts to repeat the packet drop may well occur while the token bucket is exhausted of burst credits. The time to repair from the initial overshoot may involve multiple round trip times and multiple unsuccessful retransmission attempts. These days it's important to understand that increasingly the internet is a world of streaming flows and increasingly its across mobile access networks where rate policing is common event. Google has developed the "BBR" congestion control algorithm that attempts to seek high throughput by probing available bandwidth and Round Trip Time sequentially, and attempts to control the flow within the max bandwidth window. I'd like to examine this algorithm in more detail in another article, but the bottom line is that Google are advocating its use in place of Cubic and have been using it is its own services as a means of improving the efficiency of flows in rate policed networks. (More details of the BBR approach are at http://queue.acm.org/detail.cfm?id=3022184)

While much of the world is constructing IPv6 in a dual stack context, where there is both IPv4 and IPv6 available to the applications, some environments do not treat both stacks equally. When a network deploys NAT64, or approaches that use 464XLAT, the basic approach is to always use IPv6 is there is an IPv6 address record for the service attachment point, and only to use IPv4 only if there is no signs whatsoever of IPv6. This is subtly different to the Dual-Stack Happy Eyeballs approach which in essence could be viewed as an attempt to connect using IPv6 with IPv4 as Plan B. In NAT64 and 464XLAT there is no Plan B. A survey of the Alexa site list appears to point to IPv6 DNS problems in some 2.5% of these sites (http://www.employees.org/~dwing/aaaa-stats/). Sander Stefann has been looking for sites where there is an IPv6 address record in the DNS, but the address record is either a badly constructed IPv6 address, or an otherwise good IPv6 address that is unreachable. His presentation promoted a service, nat64check.go6lab.si, that checks a service point against IPv6 issues in both the DNS and in connectivity.

There is no doubt that the Internet of Things is quickly turning into the Internet of Maliciously Stupid Trash, and a security panel focused on this topic painted a very bleak and disturbing picture.

Tim April's slide in the IOT Security Panel Session

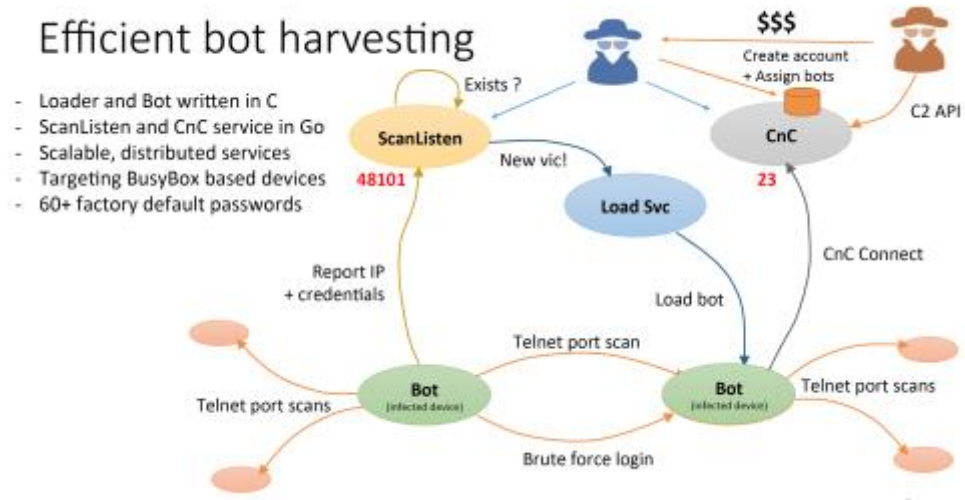
IoT Security, assuming that the two concepts can even sit together in the same breath, is a picture of poor security practice and constant scanning to detect the vulnerable. The resultant exploitation botnets are mutating quickly in line with evolving command and control structures, but the base exploit of the devices is relatively constant. The "opportunity" or case for acute depression is that the population of these devices is now outnumbering those devices that are directly controlled by humans, such as laptops, PCs and even smart devices (it's unclear whether these hermetically sealed devices are really 'controlled' by their owners, but let's put them on the human-operated side of this taxonomy). These number some 7 billion or so devices on today's Internet, equalling the roughly 7 billion 'other' connected things that inhabit the same network. The issue for growing concern is that the human device population is showing distinct signs of market saturation, whereas the world of network things is just gathering market momentum. How do we control the quality of the network security of our refrigerators, thermostats, webcams, or televisions? To the consumer that are simple devices that require power and little else. but as unmanaged devices with potential vulnerabilities their sheer numbers represent a massive issue in terms of the attack surface of the network. We already understand that the large attacks in late 2016 were the result of exploiting the vulnerabilities of the Unix engine behind a number of kits used to build consumer web cameras. The result was a scale of DDOS attacks that reach into the Tb scale. The response has been, to some extent encouraging in so far as the vendors of this equipment have appeared to be somehow immune from any liability until now. In January the FCC has taken D-Link to court in the United States for not having taken reasonable steps to secure its routers and cameras. D-Link is protesting its innocence of course, but the basic premise is that D-Link failed to take reasonable steps to address well-known security exploits. But this is perhaps a drop in the ocean and the myriad of vendors in a global market appears to completely overwhelm the limited capacity in any single national market to regulate the channels of supply and create elevated levels of care and responsibility over consumer product. NANOG may attract some 1,000 attendees, but Defcon is now 20 times larger. The Internet's obvious insecurity is now a spectator sport, and the pleas for industry self-regulation as an effective response appears to be far less than even merely palliative! The emerging state of the supply side is also a cause for concern, given that this is an industry running on a high clock speed of product design, production and distribution using globally distributed channels, coupled with the use of commodity components assembled with the lowest possible margins all points to a market failure for security. If consumers do not discriminate on such attributes and are unwilling to value them in the product and regulators are unable to control the quality of the product or hold the distributors liable then the result is a clear instance of market failure.



Jesse Sowell's slide in the IOT Security Panel Session

The questions this raises concern where this could be corrected in some fashion, and how pressure could be placed on the supply chain that would result in a natural incentive for better security practices in such devices during their entire service life. There is also the risk of political hysteria labelling everything as "critical infrastructure" and then imposing large costs and little in the way of benefit onto the industry! Hysteria is often unhelpful and especially so in this context. Time to bury our collective head in our hands, find a sheltered dark corner and cower there.

Continuing the theme of insecureware, Ron Winward of Radware presented a session on Mirai, otherwise perhaps now known as "the celebrity of botnets!" or, perhaps, the universal botnet for the rest of them! Mirai was a command and control botnet where the code was released in September 2016 on hack forums.



From Mirai: The Inside of an IoT Botnet, Ron Winward, Radware

The observation was that Mirai was nothing novel, and the code has conventional components of infection and then attack execution. The bonnet scans port 23, yes the telnet port, and attempts to perform a simple dictionary username/password scan to attempt entry. The fact that there are hosts out there with open telnet is bad enough, but that there are hosts with both open telnet and pre-set usernames and passwords is indeed scary bad! But, evidently the BusyBox devices appear to have this vulnerability in ways to many cases! The infected device then listens on port 4801 for attack control commands. There are nine attack vectors in the Mirai code, none of whic h are all that novel. The SYN

flood, ACK flood and the DNS query flood are part of this set. The fact that there are so many such open devices that can be corralled into a zombie army implies that each device is not coopted to send intense attack track individually, so at the edges this is a botnet that can be challenging to isolate and capture. What also presents challenges is that once the source code was released, the immediate response was to modify elements of the code and deploy variants of the Mirai approach.

On the topic of neat hacks I liked the lightning talk of using wireline packet capture and fast analysis. The code captures BGP packets on the wire and dumps a JSON output of the BGP content. It disconnects the monitoring process of the BGP session from the BGP speaker itself, and allows considerable flexibility in how the monitor is configured and how to process the data. I was taken with the ability of the tool to answer specific questions from looking at the BGP stream, such as the example to output the hold timers of the BGP peers at an exchange. (https://github.com/de-cix/pbgp-parser)

The meeting also included a conversation with a number of folk from the US FCC. The past few years have been somewhat turbulent times while the FCC considered the reclassification of Internet Service Providers under Title II of the US Telecommunications Act, under what was called "Network Neutrality". By all appearances the final ruling was to some extent an ersatz classification with apparently a set of exceptions and some form of undertaking to apply Title II sparingly to Internet Access Providers. With the changing of the guard in Washington the new incarnation of the FCC appears to have a commission which is leaning towards an even lighter regulatory touch. What I found interesting is that the regulatory structure in the United States, and probably many other countries as well, treat carriage as a "special" domain of activity in terms of public oversight, while the business of content is a matter of attention by regular commercial oversight and regulatory bodies. Itr should also be remembered that the impetus for the Network Neutrality debate was a difference of opinion between carriage and content providers as to the rights and conditions of access of content in these carriage networks. In other words, it was as much a content issue as it was a carriage issue.

These days the role of the Content Provider appears to be pressing closer and closer to the end user, largely eliminating the transit carrier that historically sat between the access networks and the content feeds. Another way to look at this change in the structure of the infrastructure of the Internet is to observe that much of the "haulage" component of the carriage function is now privatised and falls within the content feeder networks that are privately held and operated facilities. Presumably, such facilities fall outside of conventional FCC oversight, and it's not exactly clear to what extent this emerging domination of the Internet by content delivery systems falls under any particular public oversight. Once more it appears that our regulatory structures and the institutions that they use to conduct their responsibilities are lagging the rather more nimble private sector.

It is probably going too far to say that this content distribution sector is operating in a regulation-free zone, but their combination of multi-national span, enormous market size and influence and significant span of customers that reach across the globe is posing new regulatory questions. Is the Internet a topic for the FCC or perhaps the FTC in the years to come? It should be remembered that there is a quite significant difference in perspective between these two bodies. The FTC's mission is, to quote their web site: "To prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity." The FCC's mission is more activity-focussed: "The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the commission is the United States' primary authority for communications laws, regulation and technological innovation." It seems right now that the Internet is not behaving itself, and has changed to the extent that it is now resisting being neatly bundled into one regulatory framework or the other!

As we've come to expect from NANOG and their Program Committee, this was another excellent meeting, and I found the presentations and conversations highly interesting.

The meeting agenda, slides and YouTube presentations of all the NANOG69 sessions are linked at https://www.nanog.org/meetings/nanog69/agenda

Author

Geoff Huston B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

www.potaroo.net

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.