The ISP Column
A column on things Internet

November 2022
Geoff Huston

Going Dark

I'd like to reflect on a presentation by Dr. Paul Vixie at the October 2022 meeting of the North American Network Operators Group (NANOG), on the topic of the shift to pervasive encryption of application transactions on the Internet today.

There is a view out there that any useful public communications medium needs to safeguard the privacy and integrity of the communications that it carries. In the postal system the envelopes were sealed shut, and in the telephone system the ability to tap into conversations was a role that was often managed by some formal process involving warrants and some level of legal oversight. If you want a public communications system to be useful for the public to use, then it's necessary for the system to respect the privacy of its users.

The same applies to the public Internet, even though it has been rather loosely implemented up until now. Things are changing with respect to the privacy of network transactions, and the time when open protocols ("open" as in unencrypted clear text) represented an acceptable compromise between efficiency, speed and privacy are over and these days all network transactions in the public Internet need to be protected by adequate measures to enforce privacy, such as encryption of the transaction as it is passed over the network.

On the other hand, this deliberate occlusion of the transactions that occur across the network from the network itself is not without its attendant costs, and Paul talked about these costs in a presentation at NANOG 86 on "Going Dark: catastrophic security and privacy losses due to loss of visibility by managed private networks".

As Paul points out: "Effective modern site security is behavioural in nature. We cannot choose or exclude our endpoints nor validate their supply chains, and so to the extent that we manage digital risks posed by our endpoints we do it by watching the signals (packets and flows) they emit." What Paul is saying here is that we have to live in an environment where not all network traffic is benign. Now we can either say "it's every host for itself!" or we can try and create partitions within the network, such as a home network, or an office network, and then attempt to filter out all malicious and unwanted traffic from entering into that partitioned space. Given the ubiquity of firewalls across the network, this reliance on traffic monitoring as an integral part of site security is a fundamental assumption in today's networked environment. Unfortunately, it's an increasingly poor assumption.

As Paul observed, several decades of unapologetic abuse by the powerful have led the IETF to reform the basic Internet protocol suite to integrate end-to-end privacy in their basic operation. There is the Transport Layer Security protocol with Encrypted Client Hello, DNS over HTTPS, and the replacement of TCP by the QUIC protocol. In this new extensively obscured configuration, no firewalls or monitoring points, nor any inspection by network operators are able to detect endpoint behaviour changes corresponding to infection, takeover, poisoned software update, latent design dangers, corruption, or hundreds of other well-understood digital harms. Paul's concern is that many such operators and security equipment vendors have not been adequately warned about this change to the environment conditions and perhaps it’s time to have their expectations explicitly and immediately reset so that they can make new plans which will be practical in the next era.

The issue today is that the attackers are at a distinct advantage, in that defenders have to defend the entire space all of the time, while the attacker needs only to exploit a single weakness at a single point in time. The economics of this asymmetric situation lie firmly on the side of the attacker. And of course, these days what's at stake is much of the entire fabric of modern society.

Part of the reason why we've landed in this situation has a lot to do with the IETF's reaction to the Snowden disclosures from 2013. The general principle that pervasive monitoring is an attack, as espoused in RFC 7258, because somewhat perverted into the principle that all and any form of network level monitoring of traffic and transactions is an attack. Endpoints should be able to speak to other endpoints in an entirely private manner and no party in the middle should be privy to any such conversation. Admittedly, Paul Vixie in this presentation is taking an extreme view, but he interprets this situation as one that is tantamount to declaring "malware has rights!". Devices can sit on a home network, such as a smart television, or a baby webcam monitor or a digital watch, can operate in a manner that is completely opaque to all forms of local monitoring and control.

Compounding this is creeping featurism and ballooning complexity. The compounding of this complexity is at a pace that we simply cannot match as individuals or as an industry, and the resultant networked environment defies most form of dynamic analysis. This has a number of corollaries, particularly as it applies to site defence. Is the principle of identifying and blocking "bad" network traffic an option any more? However, is the principle of blocking everything except that which is positively identified as "good" even viable these days given the paucity of available information for a network monitoring device? What is our approach to security when firewalls cease to be effective? Do we really believe that we can make drastic improvements in the resilience of end system software stacks that can alter the rather bleak picture we have today? And if we think this is an unrealistic aspiration then what is our common security stance moving forward? Or have we been outmanoeuvred? Is the situation perhaps far more bleak than we had thought?

The conclusions Paul has reached here is that the increasingly dark network is creating some pretty ugly choices for site security administrators. There is no clear way to detect intrusion, exfiltration, malware, DOS, or any other form of abusive traffic without resorting to deliberately interposing on the end-to-end model and placing application-level proxies on the path to allow site level traffic inspection as a condition of entry and exit with the site.

As disturbing as this is, it’s not the full picture. Is the situation we find ourselves in today even more insidious than just the inability of the network to firewall filter malware and bad behaviour. We’ve changed the set of actors who can see behind the cloak of encryption. Are we letting the makers of end applications and servers to decide on our behalf who gets to see our information? Or are we in an even more extreme situation than that? Have we passed all of our information over to these large-scale players in the surveillance economy and given their absolute control over it, without any further constraints or conditions? In shutting out governments from looking over our collective shoulders have we instead run straight into the embrace of an even worse and far more insidious model of digital stalking in the guise of surveillance capitalism? Do the application providers such as Meta or Google have access to data about us that we ourselves were never privy to in the first place?

In the shift to shut out all forms of observation and monitoring have we ourselves become collateral damage here? Not only are we handing our digital assets to the surveillance behemoths, we also don't really understand what assets we are handing over, and nor do we have any practical visibility as to what happens to this data, and whether or not the data will be used in contexts that are hostile to our individual interests.

I have to share Paul’s evident pessimism. Like many aspects of our world these days, this is not looking like it will end all that well for humanity at large!

Disclaimer

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

Author

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

www.potaroo.net