March 2018
Geoff Huston

Crypto Zealots

I've been prompted to write this brief opinion piece in response to a recent article posted on CircleID by Tony Rutkowski, where he characterises the IETF as a collection of "crypto zealots" (http://www.circleid.com/posts/20180225_humming_an_open_internet_demise_in_london/). He offers the view that the IETF is behaving irresponsibly in attempting to place as much of the Internet's protocols behind session level encryption as it possibly can. He argues that ETSI's work on middlebox security protocols is a more responsible approach, and the enthusiastic application of TLS in IETF protocol standards will only provide impetus for regulators to coerce network operators to actively block TLS sessions in their networks.

Has the IETF got it wrong? Is there a core of crypto zealots in the IETF that are pushing an extreme agenda about encryption?

It appears that in retrospect we were all somewhat naive some decades ago, when we designed and used protocols that passed their information in the clear. But perhaps that's a somewhat unfair characterisation. For many years the Internet was not seen as the new global communications protocol. It was a far less auspicious experiment in packet switched network design. Its escape from the laboratory into the environment at large was perhaps more because of the lack of credible alternatives that enjoyed the support of the computer industry as it was to the simplicity and inherent scalability of its design. Nevertheless, encryption of either the payload or even the protocols was not a big thing at the time.

Yes, we knew that it was possible in the days of Ethernet common bus networks to turn on promiscuous mode and listen to all traffic on the wire, but we all thought that only network administrators held the information on how to do that, and if you couldn't trust a net admin, then who could you trust? The shift to WiFi heralded another rude awakening. Now my data, including all my passwords, was being openly broadcast for anyone savvy enough to listen to, and it all began to feel a little more uncomfortable. But there was the reassurance that the motives of the folk listening in on my traffic were both noble and pure. They twiddled with my TCP control settings on the fly so that I could not be too greedy in using the resources of their precious network. They intercepted my web traffic and served it from a local cache only to make my browsing experience faster. They listened in to my DNS queries and selectively altered the responses only to protect me. Yes, folk were listening in on me, but evidently that was because they wanted to make my life better, faster, and more efficient. As Hal Varian, the Chief Economist of Google, once said, spam is only the result of incomplete information about the user. If the originator of the annoying message really knew all about you it would not be spam, but a friendly, timely and very helpful suggestion. Or at least that's what we were told. All this was making the Internet faster, more helpful and, presumably by a very twisted logic, more secure.

However, all this naive trust in the network was to change forever with just two words.

Those words were, of course, "Edward Snowden".

The material released by Edward Snowden painted the shades of a world that was based on comprehensive digital surveillance by agencies of the United States Government. It's one thing to try and eavesdrop on the bad people, but it's quite another to take this approach to dizzying new heights and turn eavesdropping into a huge covert exercise that gathers literally everyone into its net. Like George Orwell's 1984, the vision espoused

within these agencies seemed to be heading towards capturing not only every person and every deed, but even every thought.

It was unsurprising to see the IETF voice a more widespread concern about the erosion of the norms of each individual's sense of personal privacy as a consequence of these disclosures. From RFC 7258:

> "Pervasive Monitoring (PM) is widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol metadata such as headers. Active or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols can also be used as part of pervasive monitoring. PM is distinguished by being indiscriminate and very large scale, rather than by introducing new types of technical compromise. The IETF community's technical assessment is that PM is an attack on the privacy of Internet users and organisations."

The IETF took the stance that it "will strive to produce specifications that mitigate pervasive monitoring attacks."

Strong stuff indeed. It certainly seems as if the Internet is sealing up its once very loose seams. The network that carries our packets is no longer a trusted associate that enables communications. It is instead viewed as a toxic hostile environment that simply cannot be trusted. And if it cannot be trusted then no information should be exposed to it, and all transactions should be verified by the user.

It also seems that this message is finding receptive ears. We've seen programs such as Let's Encrypt that bring the price of domain name public key certificates down to a base of free. As a consequence, secure web services are no longer an esoteric luxury but an affordable commodity. And we are now seeing one of the most popular browser in today's Internet voicing an intention to emblazon open web pages as "insecure" (http://www.zdnet.com/article/google-tightens-noose-on-http-chrome-to-stick-not-secure-on-pages-with-search-fields/). The same browser will also prefer to use an encrypted transport wherever and whenever possible (QUIC) concealing not only the payload, but also the entirety of the transport protocol from the network. It seems to be the case that about the only protocol that has a hope of passing a packet across the Internet lies in the secure payload of a TLS session, and this has not escaped anyone's attention. A good starting position is to use port 443 (HTTPS). A better position is to use QUIC. Not only is the payload encrypted, but the entire transport flow control is covered by the veil of encryption.

But the chorus is not one of universal acclaim for these measures. Some folk have not only become accustomed to a network that spewed out information, but they rely on it. As Tony Rutkowski's article points out, there is an entire world of middleware in our networks that relies on visibility into user traffic that extends right into individual sessions. Even so-called secure sessions are vulnerable (https://blog.cloudflare.com/understanding-the-prevalence-of-web-traffic-interception/). Various network-level DDOS mitigation methods rely on the ability to identify malicious or otherwise hostile traffic patterns within the network. It seems that many network operators see it as some kind of right to be able to inspect network traffic.

> This is not a recent development. When Australia was first connected to Europe in 1872 via the overland telegraph, telegrams to and from the United Kingdom were outrageously expensive. A thirty-word telegram cost the same as three weeks average wages. Little wonder that the press, a major user of the service, took to using code to improve the compression rate and at the same time attempt to hide their messages from their press rivals. The reaction was perhaps entirely predictable: all codes and ciphertext were banned from the Australian telegraph service.

Will the widespread use of robust encryption destroy any form of content caching in the network? This seems unlikely. For example, while it's true that third party content caching is frustrated by session encryption, that does not mean that content is no longer cached. What has happened is the rise of the content distribution network, where the content caches are operated by the original content publisher or their accredited agents. The user has a result of local content delivery coupled with carriage encryption and the ability to validate that the material being provided is genuine.

Perhaps the more critical question is whether the uptake of encryption imply some dire predicament for government security agencies? This outcome also seems unlikely. There is little doubt in my mind that those who have a need to worry about eavesdropping already use encryption as a matter of course. It seems that the concern from these agencies is not about having a clear window on the online activities of obvious targets, but the desire to see across the entire online environment and harvest from this larger pool of data patterns and inferences that can be analysed.

And therein lies the tension. Individually, we still value some semblance of personal privacy. We'd like to protect our digital credentials, if only to secure ourselves against theft and other forms of personal damage. At the same time, we'd like to ensure that agencies who have a protective role in our society are able to operate effectively and gather intelligence from online activities. But where do we draw the line? Should we be forced to eschew online encryption and revert to open protocols simply to feed the unquenchable thirst of these agencies for more and more data about each and every online transaction? Or should we be in a position to trust that our communications are not openly available to anyone which the means and motivation to peer into the network?

There is no doubt that the current technology stance, as espoused in the IETF, is weighted heavily on the side of privacy. We can expect more use of TLS, more use of obscured transport protocols such as QUIC, and far more paranoid behaviour from applications who no longer trust the network. Trust, once eroded, is fiendishly difficult to restore, and in this case the network has lost the trust of the applications that operate across it and the trust of the users that drive these applications. I suspect that the case for winding back the level of encryption at the network layer is long gone, and it's not coming back anytime soon!

However, I also suspect that the intelligence agencies are already focussing elsewhere. If the network is no longer the rich vein of data that it used to be, then the data collected by content servers is a more than ample replacement. If the large content factories have collected such a rich profile of my activities, then it seems entirely logical that they will be placed under considerable pressure to selectively share that profile with others. So, I'm not optimistic that I have any greater level of personal privacy than I had before. Probably less.

Meet the new boss. Same as the old boss.

> The Who's song, written by Pete Townshend, *Won't Get Fooled Again* was first recorded as part of the aborted LifeHouse project in early 1971. It was re-recorded with a synthesizer track in April 1971 and released as a single and on the *Who's Next* album in August 1971. This song formed the climax of their stage set. This song is about as old as the Internet!

Disclaimer

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

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