ARTICLE

ASTAARA COMPANY LIMITED

Securing 5G networks: All aboard the mystery train

SUMMARY

Not a panacea, but a good start. But you still can't trust it

The imminent arrival of 5G networks in the UK and elsewhere has been greeted with both anticipation and caution. The premise is a good one: ultra high-speed networks using local infrastructure, able to configure themselves for optimal delivery depending on the content – this is all great and should be applauded.

There is no doubt a lockdown behind the scenes in order to make 5G secure as possible, and none of us will have missed the global debate about whose technology can sit where in the infrastructure. But the old adage still holds true: the more nodes and access points on a network, the easier for a bad actor to get access.

Detail

The recent ENISA publication[1] on the threat landscape for 5G is helpful in spelling out how the network will be configured and structured. But on security, it was light. It goes through a number of possible attack vectors, but leaves the reader little the wiser – we will need real examples in the future if we are to avoid the lowest common denominator approach.

Despite the absence of detail, there are themes that can be usefully extracted from the report for deployment in the marine and other contexts.

1. ***Personal Cyber Hygiene***
   The importance of personal hygiene: data speeds will be much quicker than hitherto, and correspondingly larger amounts of data will be uploaded as well as streamed across the network. Strong multi-factor authentication will be vital.

   Network operators will have to be vigilant that their clients are not accidentally passing on malware for another user or into the core of the system.

2. ***Compromised Networks***
   As with its 4G and 3G precursors, one has to assume that the network itself is compromised. On that basis, it doesn't really matter what one thinks of the security architecture of 5G infrastructure.

   Since we cannot completely assure ourselves that it is not been compromised, we have to operate on the basis that it has been compromised, and therefore encrypt at the data level first.

3. ***Software***
   There is one overriding characteristic of the new 5G network: 'software defined' which essentially means that the system is not dependent on particular pieces of equipment (transmitters, phones, pagers etc). Rather it will all be about the software.

   And since there will be a lot of code in the system there will be errors and holes. Code by its very nature is buggy (one statistic quotes there being seven mistakes for every hundred lines of code in a normal everyday operating system).

5G and Shipping

It remains to be seen how appropriate 5G will be for the shipping industry. It works in cities because of the number of buildings and the ability to create micro-cells with their own mini transmitters. In rural areas as much as on the wide blue yonder, it could well be pretty much business as usual, with ships providing limited satcom access for their staff through the welfare systems.

---

[1] ENISA THREAT LANDSCAPE FOR 5G NETWORKS PUBLISHED NOVEMBER 2019 https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

There will still need to be confidentiality, but also the cost of bandwidth will be a major factor. On entering port, the vessels will clearly have to be able to hook into the 5G network of city they are visiting. There will need to be appropriate codes of connection safety rules between the domestic welfare network and the ships operation.

Given the novelty of 5G, it is to be expected that there will be significant bugs in the system, particularly in the early releases, which will have an impact on security. As with all things infrastructural, it will be for the National Technical Authorities (e.g. NCSC), the regulators (e.g. OfCom) and the telecoms operators concerned to identify and agree the minimum security standards necessary for bringing 5G into operation.

Astaara's view

Our advice therefore is that more care should be taken in the early months and years, and that companies should ensure they have redundancy built into their systems so that other networks can be invoked should 5G drop. This posture allows resilient users to remain capable of functioning, irrespective of which network is operating at the time.

I'm all for the improved ubiquity offered by 5G networks, their increased data rates, and greater access. This must be welcomed and recognised as a significant leap for connectivity. Users however need to be cautious in the early years as bugs are ironed out. Defence in depth will need to remain the order of the day

In the future the merchant marine industry will need to cover the multivariate network architectures that will be used landside, and understand their implications for Operational Technology (OT) establishments internally. Ships will need seamlessly to switch from infrastructure to infrastructure as they transit the globe.

As data rates become cheaper, shipowners will need to decide the optimum levels of connectivity for staff welfare and ship management balanced against the risks of unfettered data ingress becoming a vector for malware into the rest of the ship.

This matters not whether it's 5G, 4G, 3G or carrier pigeon: shipowners and charterers need to understand the risks inherent in enabling more internet connectivity across multiple vessels and manage that risk accordingly.

William Egerton
6th January 2020

Contact

Robert Dorey: robert.dorey@astaara.co.uk +44 (0)7775 515 878

Bill Egerton: william.egerton@astaara.co.uk +44 (0)7747 051 806

#AstaaraCyber #ResilienceandRecovery #marinecyber