fieldfisher

Codes of Practice on network security under the Telecoms Security Bill

4 December 2020

Direction of travel for MNOs and fixed line operators

Codes of Practice on network security under the Telecoms Security Bill - direction of travel for MNOs and fixed line operators

Many of the government policy discussions on 5G have centred on ensuring the economic benefits for the UK of constant connectivity are not eroded by concerns about network security. Last week's publication of the draft Telecoms Security Bill (TSB) appears to signal that operators will face both increased scrutiny over their security practices and OFCOM-issued codes of practice. In this article, we consider some of the key risks identified by the National Cyber Security Centre in January this year (in particular virtualisation of networks and the threats posed by signalling systems), what steps OFCOM may take in respect of related codes of practice for network security and whether the TSB can minimise network security issues without curbing innovative network solutions.

National Cyber Security Centre Summary of TSRs

The National Cyber Security Centre (NCSC) published its security analysis for the UK telecoms sector in January 2020 (following the July 2019 DCMS review which promised enhanced telecoms security requirements (TSRs) and putting the TSRs on a statutory footing). As part of its guidance, the NCSC made a number of recommendations about the types of security risks the TSRs ought to mitigate:

1. **Virtualisation of networks**: over time, more network functionality will be provided via software and virtualised infrastructure. Security compromises of the virtualisation fabric could impact on networks availability and, as a consequence, the NCSC recommended that the TSRs focus on best practice network architecture design.
2. **Exploitation of signalling systems**: measures must be taken to increase the resilience of networks to disruptive attacks from external signalling networks. The NCSC highlighted that the assumption that signalling from other networks can be trusted is no longer valid.
3. **Exploitation of an operator's management plane**: the critical management functionality of networks will need to be segregated from any networks with direct access to the internet as it is a prime target for security attacks.
4. **Supply chain risk**: there are a number of risks associated with equipment quality and security, supply of network access solutions and support and risks concerning operator data (including the supply of SIM cards).
5. **Loss of national capability to operate UK networks**: the NCSC highlighted the long-standing concern about the ability of UK networks to continue to operate without significant disruption in the event that removal of an individual high-risk vendor from the network was required. This issue was discussed at length in Parliamentary Select Committees immediately prior to July's decision to require UK operators to completely remove Huawei from their networks by 2027.

In the following sections, we consider the rights given to OFCOM to issue Codes of Practice on network security and the extent to which the draft Telecoms Security Bill and the existing OFCOM regime deal with virtualisation of networks and the threats posed by signalling systems (i.e. the first two risk areas highlighted above).

Codes of Practice and Security Specifications

One important question for the industry in respect of OFCOM's ability to require compliance with new Codes of Practice is the issue of standardisation of security specifications.

Codes of Practice on network security under the Telecoms Security Bill

Existing OFCOM General Conditions

Condition A2 of the existing OFCOM General Conditions of Entitlement establishes a hierarchy of standards and specifications with communications providers required to comply with the relevant compulsory standards and/or specifications listed in the OJEU for the provision of services, technical interfaces and/or network functions. In addition, communications providers are to take full account of:

- any relevant non-compulsory standards and/or specifications published in the OJEU; or
- in the absence of the above, any relevant standards adopted by ETSI, CEN and/or CENELEC.

In the absence of the above standards, communications providers are to take full account of international standards or recommendations adopted by the ITU, CEPT, the International Organisation for Standards (ISO) and the International Electrotechnical Commission (IEC).

Rights under the draft Bill for OFCOM to issue Codes of Practice

The setting of technical specifications and standards for 5G security is currently defined by a plethora of international standards bodies such as the 3GPP, IETF, ENISA, GSMA alongside bodies such as the O-RAN Alliance, Telecom Infra Project and Small Cell Forum for Open RAN deployments.

In the light of the rights given to OFCOM to issue Codes of Practice under the draft Telecoms Security Bill, the question remains what are OFCOM or the UK Government going to add to the efforts of these international bodies (other than to potentially make compliance with a particular international standard a statutory requirement for operators)?

The industry will be hoping that OFCOM balances the imposition of statutory obligations to comply with a certain set of standards against alternative deployment options which are available to operators. Some parts of the international standards are mandatory to implement but optional to use on the basis that operators ought to be able to decide on the level of security and the mechanisms to use to reach a particular result (e.g. network domain security such as IPsec) between the nodes of mobile networks.

One potential solution would be to require compliance with certain standards but give operators the option to deviate in limited circumstances from this standard, subject to an increase in the burden of proof that the deviation does not affect the overall security of the network. This certainly appears to be the intention behind section 105I of the draft Telecoms Security Bill, which gives OFCOM the ability to serve a notice on a communications provider to explain why it has failed to act in accordance with a particular provision of a Code of Practice.

Operators will be hoping to get some clarity on these issues (perhaps as part of the consultation process that is required by the TSB prior to the introduction of a particular Code of Practice) as the attendant uncertainty cannot help in circumstances where they need to make long-term decisions in respect of network architecture.

Virtualisation of networks

The introduction of cloud networking principles to telecoms networks has meant that over time, more network functionality will be provided via software and virtualised infrastructure. We have previously explored this topic and the virtualisation of the radio access network in our paper on Open RAN. The utilisation of cloud infrastructure has some potential benefits in terms of network security, as it enables more rapid patching and upgrades to network solutions. However, the 5G core network's use of service-based architecture, with an increased range of data and services, also presents more opportunities for cyber-attackers.

The quality of software development and testing is likely to be a key focus area for OFCOM and the Government, particularly given:

- previous OFCOM enforcement action in November 2019 in respect of network outages in O2's network caused by an issue with SGSN-MME software provided by Ericsson; and
- the historical concerns about software development practices, which were highlighted by the Huawei Cyber Security Evaluation Centre (the latest report was issued in September 2020 but covered the period to 31st December 2019).

In deploying Stand-Alone 5G, operators have a choice of: (a) standardised open RAN network architecture based on 3GPP Release 15 which caters for splitting baseband units into a centralised unit (CU) and a distributed unit (DU); and (b) an Open RAN as standardised by the O-RAN Alliance which, in addition to the split of CU and DU, also provides for the ability to deploy radio units (RU) and distributed units from different vendors with a Lower Layer Split (LLS) transported over the eCPRI protocol (see our previous paper on Open RAN for a discussion of eCPRI).

If operators deploy different vendors for radio units and distributed units, then this will give rise to additional security risks and OFCOM and the relevant standards bodies will need to address security issues such as mutual authentication between the RU and DU to ensure that no unauthorised equipment can be connected to the DU via the open fronthaul interfaces.

In terms of software development processes, we will need to wait to see whether standards such as the 3GPP SA3 Security Assurance Methodology (which comprises security solutions from several different standards organisations) and the GSMA's Network Equipment Security Assurance Scheme guidelines for software development and testing processes are put on a statutory footing. We will cover the detail of 3GPP SA3 in future blogs.

Exploitation of signalling systems

Security has been at the heart of the standards work undertaken by 3GPP for 5G with some security features being embedded in 5G network design that were absent from previous generations of mobile technology:

- stronger encryption and integrity protection algorithms to prevent eavesdropping and data modification;
- authentication of all elements of data transmission across 5G networks with authentication protocols being built in at the outset rather than being a bolt-on; and
- network slicing allowing networks and services to be partitioned and logically grouped on a customer-by-customer basis.

However, the deployment of 5G in the UK has initially been on a non stand-alone basis meaning that the security weaknesses in 4G networks will still be present (or need to be mitigated) in UK networks until stand-alone architecture is employed (where the 5G radio access network is connected to the 5G core network and does not rely on the existing 4G network).

The existing 4G LTE infrastructure has been perceived to be vulnerable as a result of flaws in the SS7 and Diameter protocol it uses to transmit service data. The key issue is that the 3G and 4G networks did not account for the possibility of an intruder inside the network or part of a roaming network. Two prime examples are as follows:

1. SS7 and Diameter lacked adequate authentication safeguards which resulted in attackers being able to, for example, impersonate requests from carriers to locate a mobile device or mimic legitimate roaming activity to intercept calls and text messages; and
2. hackers who are able to obtain a user's unique identifier referred to as an "IMSI" (International Mobile Subscriber Identity) can violate a user's privacy by tracking their whereabouts.

Stand-Alone 5G deployments may address these concerns by operating under a different trust model. Stand-Alone 5G deployments will not rely on the existing 4G core network and so additional security measures can be built into the 5G core network by design. In a Stand-Alone system, the trust model (as originally introduced in 3GPP Release 15) has evolved to one where trust decreases the further one moves from the core network. Baseband units (i.e. base stations) are separated into distributed units and central units where the distributed units (closest to the "edge" of the network) do not have access to any user data when confidentiality is enabled by operator's network configurations.

"Release 15" acknowledges that security issues exist under the inter-operator interface arising from SS7 and Diameter such as those identified above and looks to counter these by providing for inter-operator security from the very beginning. The issues concerning inadequate authentication are addressed by the network and devices in 5G being mutually authenticated and data transmission networks outside the mobile operator domain, such as Wi-Fi calling, undergoing secondary authentication.

These changes demonstrate how the 5G system is being designed with robust security in mind. However, there are still potential security risks associated with these technological developments.

For example:

- when the 5G network is not available, devices such as your mobile phone will look to switch to a 3G or 4G network. With that switch comes all the vulnerabilities of the previous generation's protocols; and
- the 5G networks use of a broader range of data and services and this means that there is an increased attack surface over signalling networks and network APIs – i.e. there are more items to target from a cyber -attacker's point of view.

These sorts of security issues are not easily fixed by the imposition of a statutory Code of Practice and arguably this is the sort of network security issue that ought to be left to the industry to resolve. The industry is already having to deal with the decision to require replacement of all Huawei equipment from networks by 2027. In following articles on this topic we will cover the extent to which network security is likely to continue to be industry led or whether, for reasons largely related to national security, the regulator's powers of enforcement under the draft TSB will come to the fore.

Contact Details

Paul Graham
Partner, Telecoms Sector Group
+44 (0)20 7861 4156
paul.graham@fieldfisher.com

James Walsh
Partner, Telecoms Sector Group
+44 (0)20 7861 4959
james.walsh@fieldfisher.com

Claire Harris
Senior Associate, Telecoms Sector Group
+44 (0)20 7861 4979
alex.harbin@fieldfisher.com

Alex Harbin
Associate, Telecoms Sector Group
+44 (0)20 7861 4602
alex.harbin@fieldfisher.com