How to make 5G security a reality: Q&A

Chris Mitchell
Royal Holloway, University of London
July 2019
me@chrismitchell.net

1. What does communication security mean for 5G, and do you think a network can really be made secure?
    - For 5G, like previous generations of networks, security covers a number of aspects including *fraud prevention* (protecting users against theft of service), *traffic confidentiality* (protecting against eavesdropping on transmitted voice and data), and *user privacy* (preventing tracking of users by monitoring and/or interfering with the mobile traffic).
    - There is a very long history of work on securing communication networks, including standards, products, and underlying research. The communications industry has abundant experience in building secure solutions. For myself, I have worked on security and cryptography for nearly 30 years. As a result of several decades of effort by the research community (government, industry and academia), there is a widely trusted (and widely used) set of standardised cryptographic techniques and security protocols that cover most foreseeable mainstream needs. Today, while security and cryptography standardisation efforts continue, much of the new work is aimed at more niche techniques. This is because cryptography is in a relatively mature state. Cryptographic standards have generally proved resilient, and techniques are in use today which were introduced some years ago.
    - The real issue in network security is in achieving the right balance between security and network cost. From a technology point of view, cryptographic algorithms and protocols exist to solve all envisaged security problems.
    - Of course, as we all become ever more reliant on mobile networks, reliability and availability of networks is an increasingly important issue. That is, there is rightly increasing attention on the correctness of implementations of network protocols, since flaws in implementation (even apparently not security-related) can lead to loss of availability, itself a security issue. Again, there are several decades of experience in evaluating the correctness of products and systems, and this is and will be exploited in enabling ever higher levels of assurance to be obtained in the reliability of telecommunications systems.
2. What about 5G security? Does it have any new and significant properties? Why is there so much discussion of it?
    - From a security technology point of view, 5G is just a new wireless standard and network. IN that sense, nothing is new. Indeed, the 5G security architecture is very similar to (and builds upon) the LTE security architecture; the main difference is that it incorporates a small number of enhanced and new features.
    - According to a recent NGMN Alliance working document, '5G is more secure than 4G, provided that [the] 5G infrastructure is securely implemented and that the risks are controlled by activating appropriate security features'. The main focus of 5G Release 15 (R15) security is to protect *Enhanced Mobile Broadband* (*eMBB*) services, that offer significantly greater bandwidth and lower latency than their 4G counterparts, and to offer enhanced user privacy by comparison with LTE. Release 15 of 5G is ready for commercial use. Release 16 (R16) and later versions will provide support for increasing numbers of vertical applications, and, of course, this will bring with it additional security features. Again, for real solutions, this is always a balance between greater security or more cost reduction; so far there are no problems that could *not* be solved given the willingness to incur the cost penalty.

3. How can industry and users gain confidence in the security of networks and systems, especially given that 5G will become so important to everyday living?
   - First it is important to observe that previous generations of mobile networks have provided reliable and secure services, and continue to do so. As mentioned already, 5G will offer improved security by comparison with LTE and before through enhanced security technology and through more rigorous levels of assurance-testing and certification.
   - Over the last 40 years, standardised techniques and processes have been developed to enable consumers to gain confidence in the security properties of IT products and systems. Of particular importance are the Common Criteria standards (ISO/IEC 15408) which specify how testing laboratories can test and certify products so that purchasers and users can be confident that (a) products do what they should, and, perhaps even more importantly, (b) they don't do what they shouldn't.
   - Gaining certification for products and systems using the common criteria approach can be very costly and time-consuming, and so new approaches are being developed by 3GPP (SECAM/SCAS) and GSMA (NESAS) to provide evaluation processes suitable for 5G products and systems.
4. Based on the security history of the industry, are there appropriate levels of experience and well-established methods to enable us to achieve a *cost-effective*, trustworthy, security solution?
   - Of course, the network and communications industry has been working on security and assurance for decades. A key message from the NGMN Alliance 5G end-to-end architecture framework is that 5G security should and does build upon the previous/ongoing work. From the point of view of assurance, the 3GPP Security Assurance Specifications (3GPP SCAS) and GSMA Network Equipment Security Assurance Scheme (GSMA NESAS) appear to be the most promising common baselines for global security assurance schemes. These approaches benefit all 5G operators by avoiding redundancy of assessment, and at the same time they do not preclude additional, operator-specific or location-centric (possibly government-assisted) security assurance testing. Of course, the work and expertise of ISO/IEC, which has a lot of product certification experience (from the common criteria, i.e. ISO/IEC 15408), should also be built upon. Different security requirements require different solutions; the whole industry is familiar with these assurance procedures – it is simply necessary to agree on a single approach and then it will be cost effective.
5. What influence will software-defined networking (SDN), network function virtualisation (NFV), and other new 5G technologies have on network security?
   - A March 2019 NGMN Alliance working paper on 5G security made the following important points.
     - The 5G core and access networks are to be functionally decoupled to create an access-technology-agnostic architecture, as before.
     - The 5G architecture facilitates faster introduction of new applications and services compared to traditional networks based on monolithic elements. The separation inherent in its layered structure still allows the use of the most appropriate industry best practice (i.e. for security or content management) at each layer.
     - Multi-layer isolation mechanisms could be introduced in order to reduce the attack surface and scope of impact. Examples include NFV boundary isolation, isolation of the NFV management and network orchestration (MANO) system, service instance isolation, security domain isolation, virtualised network function (VNF) isolation, network slice isolation, etc.
   - All this shows that with 5G, as with all new technologies, it is possible to design networks with secured solutions, and with even greater levels of security than was the case for LTE and before. Again, it is ultimately a balance with the cost.