5G Whitepaper:

5G Security Overview

1. Key message of this paper

Security is fundamental to the successful delivery of 5G networks across a wide range of industry verticals. This document aims to explain why security is fundamental to 5G, and how it is different from 2G/3G/4G security in relation to requirements, threat landscape and solutions.

Specifically, this document looks at the stakeholders of 5G (section 3) and demonstrates how security is a core driver for each group. A set of core challenges is presented (section 4) and then next steps are listed in section 5.

2. Support for the key message

The National Infrastructure Commission [Ref-01] states that securing mobile networks is "necessary to put the UK at the forefront of this emerging technology (5G)" and "critical to the growth of our economy".

The Future Communications Challenge Group [Ref-02] identified that government-funded developments will be required to demonstrate how security and regulatory requirements can be met in 5G. It is therefore vital that UK research and development is active in understanding and meeting the security challenges of 5G.

3. Stakeholders

It is important to identify the business reasons for 5G security i.e. the beneficiaries of the security. For example, GSM security had a goal of defending revenue in a model of mobile operators and independent retailers. 5G is more complex, involving a heterogeneous network access and a broader set of stakeholders (e.g. separation of application provider and network), including the following:

a) Network Operator: Motivations include protection of revenue, protecting the brand (which will include protecting consumer data in order to prevent brand damage), meeting license conditions and compliance (e.g. Data Protection), and offering customer additional services (e.g. adult content filtering, digital rights management). For commercial reasons, network operators need to maintain a differentiator as "carrier-grade" operators, capable of supporting high-availability businesses and critical infrastructure.

b) National Motivations: These include national security, protection of infrastructure and development of national/global economies. It covers:

- Support for Emergency Services Networks with particular requirements in disaster situations, including Citizen to Authority (999 and 112 services), Authority to Citizen (Public Warning Systems) and Authority to Authority (Emergency Services Network in the UK).
- Support to law enforcement such as Lawful Interception and Retained Data.

- Protection of Critical National Infrastructure: communications are increasingly integral to most other aspects of CNI such as water and power. 5G networks will also create and underpin entirely new components of critical infrastructure, such as tactile internet or remote monitors in health care and vehicle communications in transport.
- Defence of national/global economies: to provide confidence to do business securely to maintain an on-line global economy, to maintain the availability of communications as a core foundation of global trade. Includes support for legislation to protect intellectual property or digital rights.

c) Application security: Global over-the-top application providers are increasingly delivering end-to-end security which is not dependent on network-layer or network-operator security. End-to-end security encrypts as much as possible and exposes as little as possible to lower layers or outside parties. Such approaches typically deliver effectively against these organisations' own security goals and deliver effective privacy for their customers to the extent detailed in the generic terms and conditions that customers are assumed to have read and consented to. They reduce the ability of other organisations to access data and the approaches are not always aligned with the security motivations of other stakeholders in this list.

d) Individual security and privacy: A growing amount of people's lives take place online. People are storing and sending ever-increasing amounts of personal and financial data using mobile devices and networks. Cybercrime is expanding rapidly, with many people affected by and concerned about fraud and malware. These concerns support all the motivations in items (a) to (c).

It is important to keep in mind the increasingly diverse set of industry verticals which 5G must support. These provide a wide range of business drivers for security e.g. the transport vertical needs reliability, integrity and availability to prevent loss of life. Healthcare will also require reliability/integrity and there will be a focus on confidentiality. Smart cities applications will contain an increasing richness of personal information leading to important confidentiality concerns. Factories and energy are part of critical infrastructure which will need robust defence against cyber attack.

4. Core security challenges for 5G

The following security challenges must be addressed to meet the motivations of the stakeholders in section 3, and to meet the needs of the new business models (industry verticals).

i) Virtualisation, Edge Computing and Software-Defined Networking (SDN): 5G has challenging requirements for high bandwidth and low latency, delivered cost-effectively. It is already clear that 5G will be based heavily on Network Function Virtualisation (NFV), Mobile Edge Computing (MEC) and SDN. From a security point of view, there are the following key consequences:

- It will be harder to rely on physical separation and therefore there should be an underlying assumption that data at rest and in transit will be visible to other actors. For example, hypervisors have access to memory of functions they are hosting; also network attacks may mean that there will be many compromised components running in the same environment as sensitive functions. SDN is typically based on a centralised control architecture (to help reduce operational expenditure) which can introduce new vulnerabilities e.g. a compromised controller can give "root-like" access to configuration of virtualized devices under its control, leading to data loss or loss of network security.
- There will be a greater variety of configurations and topologies, which will be more dynamic. Sensitive data may be vulnerable during activities such as virtual machine (VM) migration or new VM instantiation.

- There will be increasing use of Open Source software. This introduces a new set of security challenges in terms of keeping a consistent and coherent approach to security-by-design, and prevention of deliberate security flaws.

ii) Support for privacy: There is increasing public debate about the importance of user privacy and about who should or should not have access to user content and its associated metadata e.g. IP addresses, device and personal identifiers and locations visited. The critical technical conclusion is that 5G should facilitate confidentiality where it is required and access to information where it is required. This can involve a concept called multi-context security: the ability to offer more than "hop by hop" encryption. This moves beyond two-party end-to-end encryption and instead allow "middleboxes" to access data in carefully controlled situations. There is an inherent tension here: much of the value from many 5G applications is derived from creating and using "big data" but this creates bigger privacy consequences for successful attacks, which in turn increases their motivation and resourcing.

iii) Internet of things: Security is impacted through scale: the number of devices to be authenticated will be an order of magnitude larger than at present, they will need to have a long lifetime (and security may not be easily upgraded), and they may also be built-in i.e. without human access (cars, meters, sensors). The consequences are that it will be impractical to physically swap identity or security modules (e.g. there is a discussion about the role of UICC). Low-power security will also need to be supported.

iv) Network management: This includes network assurance and optimization. Management and optimisation (e.g. traffic shaping) of networks are facilitated where carriers are able to understand key meta-data from the traffic they are conveying. Fraud management and cyber defence (e.g. against DDoS attack) will require network operators to understand the meta-data and content they are delivering. This may include external monitoring of malware and attacks. 5G is often associated with Self Optimising Networks and Artificial Intelligence: these concepts rely on knowledge of the network to increase performance. Some topics e.g. pre-caching rely on knowledge of the content to download content in advance.

v) Diversity of applications and networks (heterogeneity): To meet the range of 5G use cases (e.g. see [Ref-03] and [Ref-04]), it is clear that different applications will have different security requirements and will need different solutions. 5G contains various aspects of heterogeneity e.g. network slicing and Control and User Plane Separation (CUPS). These are increasingly seen as fundamental to 5G and introduce new security challenges e.g. separation between different network slices with different security levels.

vi) Security overheads: Security protections such as encryption, hashing and secure protocols in virtualized environments come at the expense of time and computational overheads. For instance, cryptographic solutions for secure outsourcing or access management lead to key management and computational overheads. As another example, trusted platform modules (TPMs – using secure protocols for confidentiality and authentication) seem unable to perform bulk data cryptographic operations due to their performance limitations and latency issues. Trade-offs in balancing the level of protection against the associated overheads need to be carefully considered, particularly for low-power or latency-sensitive applications. Protocols need to be looked at carefully to see if pre-computation can produce time savings.

vii) Interference: A threat to radio systems is interference. The IoT has caught everyone's imagination by the huge numbers being projected (various sources project 50 billion by 2020). This is generally seen as a good thing. However, the presence of many millions of long-lived devices may cause congestion in both licensed and unlicensed spectrum – the radio equivalent of space junk or seas full of plastic bags. To avoid this, it may be necessary to consider embedding a means to remotely switch off redundant IoT devices operating in prime mobile bands. If a means to turn them

off remotely is embedded, its security needs careful design, as it may be used to cause Denial of Service.

5. Next steps

Security is more effective when added by design from the outset, rather than as an "add-on". Security-by-default is crucial for 5G, given the depth and diversity of security challenges. It must also support evolution, such as protocol changes and algorithm choice.

This White Paper urges everyone reading this paper to engage on as many of the following topics as they can:

- Publicise the message about the importance of security to the business success of 5G.
- Drive a clear debate about the need for a balanced approach to some of the tensions identified in this paper e.g. privacy and network management (section 4 items ii and iv) and operators and application providers (section 3 items a, b and c). Engage with all parties about the benefits of avoiding a one-sided position which does not deliver for all stakeholders.
- Encourage vendors to develop products which support NFV/SDN security. Stimulate a marketplace for products which support the isolation of sensitive functions in virtualised environments, where appropriate linked to a hardware root-of-trust, as defined by NFV Security standards (such as [Ref-09]).
- Support and engage with 3GPP SA3 security protocols; TR 33.899 and the subsequent TS in December 2017 will set phase 1 issues and solutions. These groups must be pragmatic and realistic in what can be achieved in the timescales, but we must not miss opportunities to bring in new material where it is crucial to the success of 5G.
- Engage with members of Open Source communities and advocate the need to bring more security into Open Source. Identify early opportunities to include code (starting in a small way) which helps address any of the security challenges in this paper.
- Ensure security-by-default is built in to 5G test bed developments. The FCCG report notes that security will need to be demonstrated as part of funded 5G developments. Engage developers designing early 5G test beds and establish which security criteria can be included at the early stages.

Annex A: Standards groups

This Annex covers the range of standards groups and industry bodies working in this space at present.

Business focus: The starting point is to look at 5G groups which are summarising how operators intend to make a successful business out of 5G, and the requirements which they derive. The following papers are written by groups which have a business focus:

- NGMN 5G White Paper [Ref-03].
- 3GPP SMARTER [Ref-04] requirements, demonstrating the interests of the operators in terms of how they can benefit from migrating to 5G (these also have input from 5GPPP which includes EU Commission and research interests).

Fundamentals of 5G networking: The next layer of foundations is to examine how the 5G requirements will impact on security techniques. Detailed discussions are found in:

- ETSI Next Generation Protocols White Paper [Ref-05].
- ETSI NGP Scenarios specification [Ref-06].

Detailed research on 5G security: These groups are part of the evolving standardisation and research work on 5G security:

- 3GPP 5G Security group SA3 (for example through the report [Ref-07]). Work at the architecture group SA2 (see report [Ref-08]) will also have an impact. The focus of security work is SA3 and the related work in SA3-LI and ETSI TC LI.
- NGMN White Paper on Security for Network Slicing [Ref-12].
- Security standards from ETSI ISG Network Functions Virtualisation (NFV), specifically GS009 looking at multi-layer security [Ref-09] and also [Ref-11].
- 5GIC paper: “Subscriber Data Management Security for Flat Distributed Cloud” [Ref-10].

Groups which are strongly related to 5G security: The following groups are important to 5G security though not specifically focussed on 5G per se:

- ETSI TC CYBER – work item on middlebox security protocols.
- ETSI ISG MEC: Mobile Edge Computing is likely to be a core technology for 5G to deliver the latency requirements.
- 5G Ensure, a EC project under the Horizon 2020 project – see [Ref-13].
- GSM Association Fraud and Security Group – see [Ref-14].
- IoTSF – The Internet of Things Security Foundation – see [Ref-15].
- Trusted Computing Group.
- Though not specifically 5G focussed, there will need to be an increased effort on malware reporting such as via the Structured Threat Information eXpression (STIX).
- Open source communities e.g. OpenStack.

Future research on 5G security can look to create a full analysis of the state-of-the-art in terms of industry solutions and academic papers.

References

Ref-01: National Infrastructure Commission: Report into 5G and telecommunications technology, December 2016: https://www.gov.uk/government/publications/connected-future.
Ref-02: Future Communications Challenge Group Report, December 2016: https://www.gov.uk/government/publications/interim-report-of-future-communications-challenge-group-uk-strategy-and-plan-for-5g-digitisation.
Ref-03: Next Generation Mobile Networks (NGMN): 5G White Paper, February 2015.
Ref-04: 3GPP TR 22.861, 22.862, 22.863 and 22.864: "SMARTER 5G requirements"
Ref-05: ETSI Next Generation Protocols White Paper.
Ref-06: ETSI Industry Specification Group for Next Generation Protocols (ISG NGP): GS 001 ("NGP Scenarios")
Ref-07: 3GPP TR 33.899 from SA3 (still in draft): https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045.
Ref-08: 3GPP TR 23.799 from SA2.
Ref-09: ETSI ISG Network Functions Virtualisation (NFV) specification GS-SEC-009 ("Multi-layer security").
Ref-10: 5GIC paper: "Subscriber Data Management Security for Flat Distributed Cloud", January 2016.
Ref-11: "ETSI Group Specification: Network Functions Virtualization (NFV) NFV Security and Trust Guidance," Dec. 2014.
Ref-12: Next Generation Mobile Networks (NGMN): 5G security recommendations Package #2: Network Slicing.
Ref-13: 5GEnsure: see http://www.5gensure.eu/
Ref-14: GSM Association Fraud and Security Group: http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group
Ref-15: IoTSF Internet of Things Security Foundation: https://iotsecurityfoundation.org.